Albladi and Weir *Hum. Cent. Comput. Inf. Sci.* (2018) 8:5
https://doi.org/10.1186/s13673-018-0128-7

Human-centric Computing and Information Sciences

RESEARCH Open Access

User characteristics that influence judgment of social engineering attacks in social networks

Samar Muslah Albladi* and George R. S. Weir

*Correspondence:
samar.albladi@strath.ac.uk
Department of Computer and Information Sciences, University of Strathclyde, Glasgow, UK

Abstract

Social engineering is a growing source of information security concern. Exploits appear to evolve, with increasing levels of sophistication, in order to target multiple victims. Despite increased concern with this risk, there has been little research activity focused upon social engineering in the potentially rich hunting ground of social networks. In this setting, factors that influence users' proficiency in threat detection need to be understood if we are to build a profile of susceptible users, develop suitable advice and training programs, and generally help address this issue for those individuals most likely to become targets of social engineering in social networks. To this end, the present study proposes and validates a user-centric framework based on four perspectives: socio-psychological, habitual, socio-emotional, and perceptual. Previous research tends to rely on selected aspects of these perspectives and has not combined them into a single model for a more cohesive understanding of user's susceptibility.

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

Introduction

Although stronger security measures are increasingly developed, promoted and deployed, the number of security breaches is still increasing [1]. This may be because cybercriminals often target a weak and easy access point, the user. No security issue can arise unless there is a weakness that can be exploited by cybercriminals [2]. Security breaches are causing significant damage to organizations in different industries through decreasing customer trust [3] and stock returns [4]. According to a report published in 2015, the estimated cost of the data breach that occurred in 2013 to Target, a retail company in the US, ranges between $11 million to $4.9 billion [5]. Furthermore, a recent study conducted by Ponemon Institute [1] states that cyber breaches among 419 organizations cost an average of $3.62 million. Using advanced and sophisticated deception methods to manipulate the user in order to access sensitive information is the essence of social engineering (SE). Most communication media, such as email, telephone, and recently social networks, have been affected by social engineering threats (Additional file 1).

Social networks are one of today's most popular communication media and attract millions of active users to share and express their thoughts, photos, and locations with others. This popularity has also attracted cybercriminals who find social networks to be a rich setting for their illegal activities. For example, social networks may be used as the main channels for cyber-bulling activities [6]. Through social networking sites (SNSs), social engineers can execute direct attacks, such as social networks phishing [7], and reverse social engineering [8], or indirect attacks, when the victims' social network accounts are hijacked to collect information that facilitates subsequent attacks in other contexts. For example, determining employees' personal information through tracking their online footprints in social networking sites [9], or by linking employees' profiles across multiple SN channels [10] which can facilitate successful social engineering attacks on their company.

Relying on social network providers to protect their users' privacy and security from cybercriminals is a common attitude among users of such networks. Those users may tend to reveal their sensitive information online without being aware of potential exploitation [11]. Social engineering attackers usually use deceptive strategies to convince their victims to accept the lure instead of exploiting technical means to reach their victims.

The risks to users persist, with a recent study revealing that only 25% of their participants have detected the phishing attacks [12]. Thus, research aiming to comprehend human activities and practices that lead to potential abuses is vital to thwart the effectiveness of any security threats [13]. Existing social engineering vulnerability studies have concentrated on variables that make human users powerless against social engineering threats, such as personality traits [14], demographics [15], and online habits [7] separately, but have never attempted to analyse their impact together in the same structure in the context of social networks. The present study proposes and validates a user-centric framework (UCF) with a view to building a coherent understanding of human susceptibility to social engineering-based attacks in the social network (SN) setting.

The present study is not the first to investigate human vulnerabilities to social engineering in social networks context but, affords novel theoretical contributions by (i) incorporating experts' opinions in determining the most influencing factors that impact upon users' threat detection abilities and (ii) combining multifaceted factors and various theories in one framework to understand human behavior when encounter online threats.

This paper is organized as follows. "Literature review" section briefly reviews the relevant literature. The method used to build the proposed framework is summarized in "User characteristics framework construction" section. Following this, the approach used to validate this framework and the methodology adopted in this work is described in "Validating the proposed UCF" section. In "Results and findings" section, the results of the analysis are discussed together with the findings. "A service scenario for using the proposed UCF" section provides a service scenario for using the proposed framework. Finally, "Conclusion" section draws conclusions from this work.

Literature review

Social engineering in social networks

When investigating human behaviour toward online threats, it is important to focus on the interaction between the individual's attributes, their current context, and the message persuasion tactic [16]. According to a taxonomy proposed by Krombholz et al. [17], the three main entities that encapsulate social engineering attacks are operator, type, and channel. The operator of the attack can be either a human or malicious software.

The type of operator can also determine the chosen type of social engineering attack. One taxonomy [18] has classified the type of attack to be technical-based, which includes phishing, scam, and malware, or human-based, such as impersonation, identity theft, and reverse social engineering. An example of a technical based attack in social networks is the cross-site scripting attack that recently become popular among criminals in SNSs [19]. In contrast, persuading the victim to contact the attacker by connecting with the victim's friends through a reverse social engineering technique [8] is an example of a human-based attack in social networks.

Context plays a critical role in social engineering attacks because this determines the complexity of the attack, especially for the operator. It has been argued that in social networking sites, there are three main sources in the user's profile that cybercriminals use to reach their victims, content, friendship connections, and privacy settings [20]. A network's privacy and security settings are important measures to protect the user. Even with the limited functionality of current social network security and privacy preferences [21], if users adjust the network's privacy setting and prevent non-friends from accessing their account, the attacker would not be able to use the account to gather the information required to conduct indirect attacks.

The receiver of the attack is always responsible for evaluating and recognising the attack in order to prevent it from succeeding. The user's ability to detect the attack is determined by a range of user characteristics. Figure 1 presents a general taxonomy of

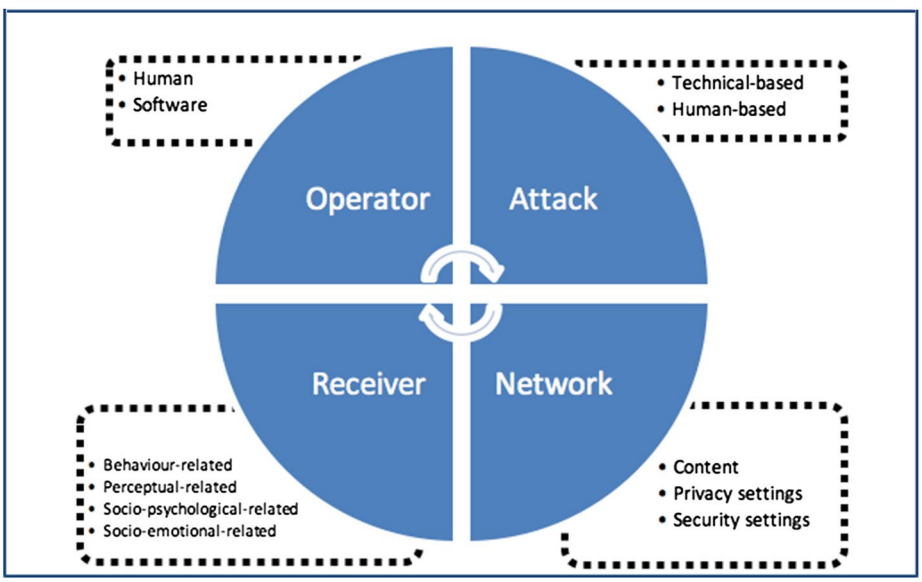

Fig. 1 General taxonomy of social engineering attacks in social networks

social engineering in social networks which is developed from previous taxonomy studies. However, among the four major entities that formulate the social engineering attacks in social networks, the present study focuses only on receiver characteristics that make the end-user more vulnerable to social engineering attacks and will be discussed in more detail in the next section.

User vulnerabilities

User vulnerability to social engineering can be defined as the set of user attributes that incline that particular user (rather than other individuals) to be a victim of social engineering attacks. Previous user vulnerability research can be divided into four groups depending on the focus of attributes that they investigated.

Behaviour-related attributes

Prior literature on email environment victimisation [22–24] has explored the effect of social network habits on predicting behaviour toward email phishing. In the virtual network setting, users tend to exhibit their trust by their degree of engagement in the network [25]. The individual's level of network engagement can be determined by a number of factors such as number of friendship connections [7], or time spent in the network [26]. High levels of social media usage have been found to make users more exposed to online threats in knowledge exchange networks [26].

A technical study [27] conducted on the Twitter platform found that profile and content related features are efficient predictors of malicious and honest users. Vishwanath [7] also examined how user habits in Facebook can predict the user's vulnerability to social media phishing attacks, concluding that user's social network habits such as frequency of use, lack of control over usage behaviour, and maintaining online relationships can anticipate social engineering victimisation and that highly-active users are more susceptible to social engineers as cybercriminals consider them more valuable. For instance, highly-active users may ensure the accomplishment of the attack as the friendship connection between the victim and the attacker may lead to the victim's friends being deceived by a reverse social engineering technique [8]. Conversely, users with fewer involvement components, such as limited number of connections and less regular use, are not the best targets for the attack in light of the fact that the lure message may not be seen at all, since the user does not utilize the SN much of the time.

Moreover, the behaviour related studies reported above do not clarify the reasons that relate the online user's habits to the phishing victimisation. One possible explanation for this relationship is that the users' online habits may affect their perceptions, on factors such as risk and trust, which in turn affect their susceptibility to social engineering-based attacks.

Perceptual-related attributes

Protection motivation theory has been taken as a theoretical foundation for many studies in the field of information security (IS). One such is Workman et al. study [28] which suggested that perceived severity and perceived vulnerability to security threats are significant predictors of users' security behaviour motivation. According to protection motivation theory in IS research [29], when a user encounters a threat, four

cognitive factors will be needed to assess the threat: perceived vulnerability (estimation of threat occurrence), perceived severity (to what extent the consequences will be cruel), response-efficacy (to what extent the protection behaviour will be efficient), and self-efficacy (assessment of individual ability to adopt protective behaviour).

Perceiving the risk associated with engaging in online activities is considered a direct influence of people suspicious of existing online threats [22]. Notably, some research found no correlation between perceived risk and users' behaviour toward either email phishing [30], or social network victimisation [26]. This contradicts the view that the individual's perceived severity of negative consequences predicts their detection or avoidance behaviour of online threats. Furthermore, some research has focused on other individual attributes such as self-efficacy [24, 30], security awareness [30, 31], and privacy awareness [7, 23], all of which play an important role in self-protection practices online. Yet, an investigation of the limitations of current SN privacy control systems suggested constructing new user-focused privacy requirements that give SN users the ability to control and protect their contents [32].

Socio-psychological-related attributes

Personality traits impact on phishing victimisation has been noticed by social engineering researchers. However, this has only indicated that specific traits may cause higher susceptibility rates and did not test whether specific demographics, such as gender, contribute to this relation.

Existing empirical studies have measured the relationship between the Big Five Personality Traits and email phishing victimisation [23, 33]. However, there are still some antithetical results as Halevi et al. [23] stated that neuroticism is the trait most correlated to responding to a phishing email, while Alseadoon et al. [33] found that openness, extraversion, and agreeableness are the personality traits that increase the possibility of a user response to phishing emails.

Furthermore, gender, age, and educational background are the most contradictory variables in the existing literature of phishing research [34] and are repeatedly examined in relation to phishing victimisation. According to the potential victim's age, some research results state that younger users are the most potential and vulnerable targets of deception. Yet, these results are difficult to generalise as the vast majority of such studies were reported on constrained samples, mainly university students [23, 33]. It was found recently that among many examined demographic features, computer usage experience, as well as gender, are the most significant predictors of user's detection ability of web-based phishing attacks [12]. Yet, in the context of victimisation in social networks, self-confidence in computer skills might lead to risky behaviour as a positive relationship has been found between higher computer skills and user victimisation [26].

Culture has been given less attention in IS research in general and in social engineering victimisation research in particular. One report on email phishing [35] has stated that some cultural value might incline people to behave in a certain way such as being trustful, or generous. Those people will be more vulnerable to phishing victimisation as they may easily be exploited if emotionally persuaded by the attacker [35]. Flores et al. [36] investigated whether culture has an impact on email phishing resistance among

employees from different nations (USA, Sweden, and India). The study result proved the significant role of culture in the users' behaviours and decision-making at times of risk.

Socio-emotional-related attributes

The attacker's persuasion techniques are various and their impact on the users' responses are diverse and related to the chosen inducement tactic, as revealed by Workman grounded theory investigation [37]. As a group of people can be persuaded by trust and friendly rapport, others can be influenced by fear tactics.

Extracting emotional-based features from a social network platform has been found to derive information useful to distinguish between malicious and honest users [27]. Other existing research [38, 39] has focused on emotional triggers, such as fear and anxiety, that incline users to react to various types of social engineering attack. Trust is one of the emotional variables that has not been given enough attention in previous research. In reality, trust is a basic component of any online or offline individual's communication and relationship enhancement. A further study [40] proposes that friendship connections reveal high accuracy as measures of trust among social network individuals. Trust in the virtual environment of social networks can be classified into two types: trusting the medium and trusting the members [41]. The density of information sharing in a social network is related to the amount of trust their users have with regards to the network providers and members [41]. Trust regularly prompts a lesser perception of risky behaviour, which eventually may raise the likelihood of succumbing to social engineering attacks.

User characteristics framework construction

Following the extensive literature review on the user characteristics that may influence the user's judgment of online attacks, several attributes have been chosen to develop a user-centric framework. To construct the framework based on existing studies and theories, the following is a summary of the steps that have been taken.

Selected attributes grouped under themes

In an attempt to build a focused and coherent framework, the selected attributes have been categorised and grouped under themes in regard to the attribute's nature.

Removing and merging overlapping concepts

When the attributes have been grouped in themes, similar and overlapping terms were obvious which allowed for the merging of some terms in order to form a single attribute. For example, computer expertise, computer experience, and email experience are related factors and can be represented under the single term 'computer knowledge'.

Framework construction

Based on the previous classification process, the framework was constructed after converting 51 terms into 14 factors. Figure 2 shows the proposed user-centric framework (UCF). Appendix A presents the definition of each factor in details.

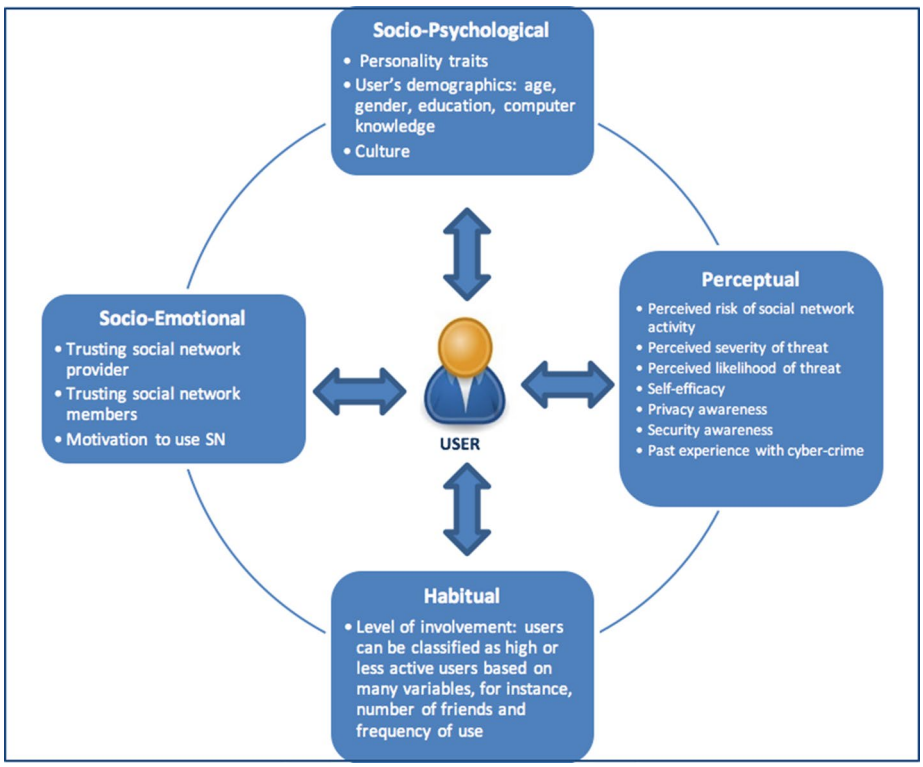

Fig. 2 User-centric framework (UCF)

Comparison of similar frameworks

Similarly-motivated and empirically tested frameworks in the literature, in email or social network environments, have been reviewed to indicate the similarity and differences between them (as presented in Table 1 where (√) indicates inclusion of the attribute in the considered model, see also [42]). From the comparison, it was clear that the socio-psychological factors have been given extensive attention by researchers in the field. Research has considered limited perceptual and habitual variables in their models, while the socio-emotional perspective and its dimensions have never been investigated before in relation to their effect on social network victimisation. Yet, in an email environment [33] and [30], have examined people's disposition to trust others as a personality adjective and its impact on email phishing.

In social network models, some variables, such as personality traits, culture, and past experience with cyber-crime, have rarely been considered to influence victimisation. Regarding past experience, Parrish Jr., Bailey, and Courtney's model [43] has proposed experience as a potential factor that impacts the user judgment. Yet, this model has still to be evaluated and, therefore, is not included in our comparison. Furthermore, in the perceptual perspective, the individual's estimation of the severity and likelihood of threats and their privacy and security awareness might be considered insufficiently investigated in previous models. Two models have indirectly studied privacy awareness and its relation to phishing vulnerability. Vishwanath [7] model has investigated the individual's privacy concerns that indirectly refer to privacy awareness, and has found this

Table 1 Comparison of similar frameworks in email and social network contexts

Attributes	Context									
	Social network environment				Email environment					
Model (year):	**[31] (2017)**	**[26] (2016)**	**[7] (2015)**	**[44] (2015)**	**[12] (2016)**	**[22] (2016)**	**[33] (2015)**	**[23] (2013)**	**[24] (2011)**	**[30] (2010)**
Socio-psychological										
Personality trait							√	√		
Age	√			√	√		√			
Gender	√				√			√		
Education				√	√					
Computer knowledge	√	√			√		√	√	√	√
Culture					√					
Habitual										
Level of involvement in SN		√	√			√		√	√	
Socio-emotional										
Motivation to use SN										
Trusting SN provider										
Trusting SN members										
Perceptual										
Self-efficacy									√	√
Perceived risk		√				√				√
Perceived severity										
Perceived likelihood								√		
Past experience										
Privacy awareness			√					√		
Security awareness	√									√

to be not significant. Likewise, Halevi et al. [23] model investigated the privacy awareness indirectly through examining the user's adjustment of Facebook's privacy settings as a pattern of the user-Facebook activity, which proved to be a significant predictor to phishing vulnerability.

The need for a multidimensional perspective has emerged after conducting this comparison. There are many significant attributes that should be considered when examining user vulnerability to social engineering victimisation. In contrast to the existing frameworks, the proposed framework affords a more extensive and robust user-centric model that provides a starting point for future studies to understand user susceptibility to social engineering in SNSs.

Validating the proposed UCF

The present study adopted expert reviews as a mixed method approach to validate the proposed framework with an objective to confirm or modify the proposed UCF. This approach is important as a means to evaluate the dimensions and attributes of the newly developed framework in order to get proper feedback and validate the proposed framework in the study context. The study detailed here was composed of two major parts: quantitative and qualitative. In the quantitative part, participants were presented with the proposed framework, asked to read each factor's description carefully and rate the importance of the framework's factors in terms of their effects on users' judgments of social engineering attacks in social networks. The qualitative part includes some open-ended questions that aim to gather the experts' opinions and recommendations to improve the proposed framework. Two rounds of experts' review were conducted in the present study in order to increase the reliability of results by using the inter-rater reliability approach [45]. This approach aims to identify the degree to which the results obtained from both rounds of the evaluation are stable and yield similar results, even though different experts have participated in each round. The results of the two rounds have been compared in order to examine whether there are any differences between the two groups in terms of the importance of the frameworks factors to identify users' ability to detect online threats. Figure 3 describes the process that has been taken to validate the proposed framework.

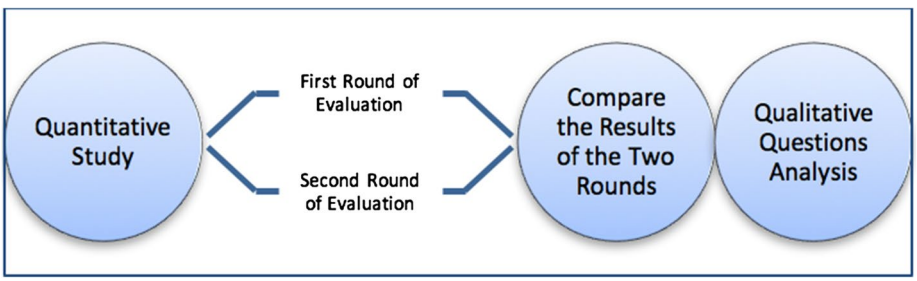

Fig. 3 Framework validation method

Instrument design

An online questionnaire has been designed which has three parts. The first part asked about participants' demographics such as their age, gender, and level of expertise. The second part includes the framework dimensions and factors. Each factor has a brief description to explain what it means in the study context. Respondents have been asked to rate the importance of each framework factor on a 5 point Likert-scale. In the third Part, participants were asked to express their opinions about the framework by answering three open questions. Completing this part was optional. The open questions asked the experts to indicate the following:

> From your experience, are there any factors in the framework that should be combined?
> From your experience, is there any factor in the framework that should be split?
> From your experience, do you think there are any other factors that should be included in the framework?

Sampling

To be included, participants required sufficient knowledge and significant experience in the information security field. Experts were selected with this in mind from universities' and organisations' websites. The selected experts were sent an email asking them to participate in the survey. In the two study rounds, 63 emails have been sent with 27 responses received, from which 11 have completed the open-ended questions. Table 2 presents the demographics of the experts who participated in the qualitative part of the study. The adequacy of using small sample in the expert review approach has been confirmed in a number of previous IS studies [45, 46]. However, in order to mitigate any residual limitation from sample size, the sample selected included both genders, a range of ages between 25 and 44 and also included different levels of education and expertise.

Table 2 Qualitative study Expert's demographics

Expert number	Age	Gender	Education	Expertise (years)
Expert 1	35–44	Male	Ph.D.	Over 15
Expert 2	35–44	Male	Ph.D.	11–15
Expert 3	35–44	Female	Ph.D.	Over 15
Expert 4	35–44	Female	Ph.D.	11–15
Expert 5	35–44	Female	Master	11–15
Expert 6	25–34	Male	Master	6–10
Expert 7	35–44	Female	Master	6–10
Expert 8	35–44	Female	Master	6–10
Expert 9	25–34	Male	Master	1–5
Expert 10	25–34	Male	Bachelor	1–5
Expert 11	25–34	Male	Bachelor	1–5

Procedure

An invitation email was sent to the selected experts asking them to participate in the study. The study was conducted in two phases. In the first phase, an email was sent to 43 information security specialists who work either in academic or other organizational sectors. 30 responses were received of which 15 completed the survey. The second phase was conducted 1 month later. An email was sent to 20 information security experts, all of whom were academic lecturers in Saudi Universities, and 12 responses were received. The reason behind conducting the second phase of experts' review with a different sample of experts is to increase the reliability of the framework's validation and the results of the first experts' review.

Analysis methods

The collected quantitative data (Additional file 1) was analysed using SPSS statistical software. Previous research provided evidence for the robustness of parametric statistics with Likert-scale data even with some sort of violation on sample size and normality [47, 48]. Therefore, the present study used one sample t-test to analyse the result for the first group and an independent t-test to compare the results of the two groups.

Results and findings

Agreement upon the framework's factors

In order to measure the sample agreement level on the framework factors, one sample t-test was carried out. This test would determine the importance of each factor in order to decide whether to keep it or remove it from the framework. Table 3 describes the mean from the five-point Likert-scale and the corresponding attitude.

Table 3 Attitude of the scale mean

Mean	Attitude	Description
1.00–1.79	Not important	The item must be excluded from the framework
1.80–2.59	Slightly important	
2.60–3.39	Moderately important	Item needs revision to be included in the framework (if the item mean is less than 3, exclude the item from the framework)
3.40–4.19	Important	The inclusion of this item is essential for the framework
4.20–5.00	Very important	

Before starting the validity stage, the data went through several screening steps to be checked as follow:

Data screening approach

The data has been checked for any missing data. One participant response was removed from the test as the participant missed 5 sequence items in the rating question which implies that this particular participant had decided not to complete the questionnaire. Furthermore, Shapiro–Wilk test has been used to check the normality of the data. Data has been found as normally distributed (sig. > .05) except for the habitual dimension (sig. = .038) in the first round and socio-emotional (sig. = .019) in the second round which considered slightly violated from normality.

According to checking careless responses, the "user's height" item has been added as a bogus item to the socio-psychological item set in order to reveal inattentive responses. Results showed that all respondents in both phases were giving sufficient attention and ranked the item as "Not important", with means 1.7 and 1.5 respectively.

Validity of the test

In order to validate the questionnaire scale reliability, Cronbach's alpha has been measured for both study phases. Cronbach's alpha for all perspectives was above .5 except for the socio-emotional perspective. According to the socio-emotional perspective in the second phase, Cronbach's alpha was only .399. Therefore, trusting items should be separated from the motivation item in order to increase the reliability to .855 as observed in the test. This implication is also supported by the findings from the expert qualitative study and this will be discussed more in the findings section.

One sample t-test

After screening and checking the collected data, the data was ready for the statistical tests. The one sample t-test was conducted with the goal to determine the sample agreement level of each item and thereby determine whether to include or exclude this item from the framework. Items with mean less than 3 are considered not important and must be excluded from the framework, as described earlier in Table 3. This decision can be taken after establishing the test hypothesis: H0: the null hypothesis ($\mu = \mu 0$); there is no significant difference between the sample mean and the population mean; which indicates that the mean of each framework factor is equal to 3. H1: the alternative hypothesis ($\mu \neq \mu 0$); there is a significant difference between the sample and population mean; which indicates that the factor mean is not equal to 3.

To test this hypothesis alpha ($\alpha = .05$) has been chosen as Support H0 if the item's sig. is greater than alpha (no difference in means). Support H1 if the item's sig. is less than or equal alpha (there is a difference in means).

Table 4 lists the one sample t-test results. Generally, the t-test results show that all the framework's selected factors are considered important in this round. In the following section, each theme will be analysed separately.

Table 4 One sample t-test (first group)

Factor	Sig.	Mean	Attitude	Hypothesis	Factor	Sig.	Mean	Attitude	Hypothesis
Per_T	.002	4.14	Important	Alternative	Trust_M	.002	4.07	Important	Alternative
Age	.003	4.14	Important	Alternative	Motivation	.055	3.57	Important	Alternative
Gender	.671	3.14	Moderately important	Null	Risk	.003	4.00	Important	Alternative
Education	.000	4.57	Very important	Alternative	Self_efficacy	.045	3.64	Important	Alternative
Comp_K	.000	4.50	Very important	Alternative	Severity	.165	3.43	Important	Null
Culture	.000	4.14	Important	Alternative	Liklihood	.045	3.64	Important	Alternative
No_frinds	.045	3.64	Important	Alternative	Past_exp	.008	4.07	Important	Alternative
Frq_use	.045	3.64	Important	Alternative	Priv_aware	.015	4.07	Important	Alternative
Trust_P	.009	3.93	Important	Alternative	Sec_aware	.000	4.43	Very important	Alternative

Findings and discussion

Socio-psychological attributes It can be seen from Table 4 that the significance value in all the socio-psychological items is less than alpha (= .05). Therefore, the null hypothesis will be rejected, except for the gender item. In this case, the alternative hypothesis will be rejected and the null hypothesis will be accepted. However, the statistic mean for this item is higher than the population mean ($\mu 0 = 3$) and has been ranked as moderately important in the scale which makes this item hard to exclude from the framework. Surprisingly, the experts did not consider gender as a very important determinant, a result that opposes many previous studies [12, 23, 31]. One of which was Algarni et al. [31] experimental study that revealed a strong correlation between gender and response to social engineering attacks in social network contexts. Moreover, it can be seen from Fig. 4 that education has the highest rank among other considered factors. This result conflicts with a previous study which argued that the level of education is not significantly related to phishing victimisation [12]. But most importantly, when comparing university students with people from outside higher education institutions [44], both behave in a similar way in social networks. Yet, students have been found to be less likely to fall victim to cyber-attacks.

Computer knowledge is considered one of the highest rated factors in the experts' assessment (Fig. 4). Yet, among many studies [12, 23, 24, 26, 30] that have empirically tested the impact of the Internet and computer knowledge in preventing users from getting phished, only two studies [12, 30] found this relation to be significant. This contradictory result might imply that user internet or computer knowledge is a very general concept whose impact on safe or risky behaviour could be hard to measure. In the qualitative study, Expert 5 mentioned that as the targets of the attacks are social network users, there is no need to measure their computer knowledge and instead, measuring the social network literacy is more relevant. Another participant, Expert 6 had a similar view as he mentioned that computer knowledge is not important if internet security and privacy awareness are measured, as all these attributes are related to each other and could be merged in one construct. Furthermore, Expert 9 stated that nowadays, social network users generally have the basic knowledge of computer usage. But the problem lies only with their knowledge of computer security.

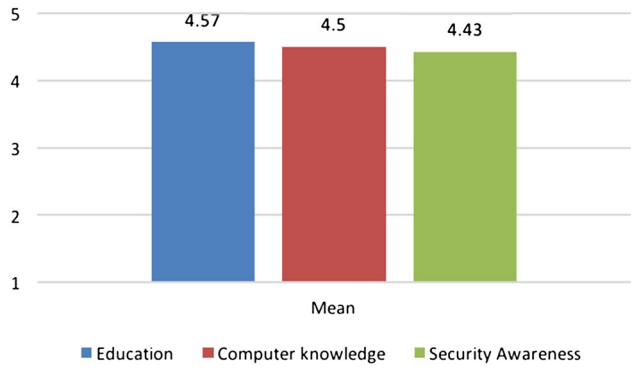

Fig. 4 The three highest rated factors

Habitual attributes The experts' evaluation revealed that habitual factors are on the importance side to include in the framework. This supports previous findings that presented the critical role of the involvement level of the user on the phishing vulnerability both in the email context [22–24], or in the social network context [7, 26].

Socio-emotional attributes Unlike the context of email, social network members play a vital role in users' trust. Table 4 shows that trusting the social network members is the factor ranked highest by the experts as causing users to poorly judge social engineering-based attacks in a social network context. Furthermore, people tend to rely on social network providers to protect them against privacy and security threats, which explains their trusting attitude online.

The socio-emotional factors, SN trust, and usage motivation were ranked as important by the experts, and this reflected the gap in the literature, as these two factors have never been encountered in previous frameworks. Although Workman model [37], Alseadoon model [33], and Wright and Marett model [30] have studied the individual's disposition to trust as a factor to affect the user vulnerability to email phishing, they did not reach the same conclusion. Workman and Alseadoon's studies have found that individuals who are more trusting would be more vulnerable to social engineering than others. In contrast, Wright and Marett's study has found the relationship between trust and deception success to be not significant. Yet, in this study, two types of trust have been proposed, trusting SN provider and trusting SN members, which are more specific to the context of social networking. However, Expert 3 suggested combining these two types of trust in one construct. Expert 8 also suggested splitting the motivation factor into multiple sub-factors as there are various types of motivations that persuade users to engage more in SN. Thus, this study proposes trust as a multi-dimensional construct that includes provider trust and member trust. This also confirms the previous findings of the reliability tests of the second group that the Cronbach alpha will be raised from .399 to .855 if the motivation item is deleted and only the two types of trust remain.

Perceptual attributes The survey results revealed that the perceptual factors are generally very important factors to consider in relation to user susceptibility to social engineering. Results shown in Fig. 4 indicate the importance of security awareness, which has been proven to be significant in previous empirical studies either in an email setting

[30], or a social network environment [31]. This importance has been emphasised by the answer of Expert 2 in the qualitative part of the study as he stated that some of the perceptual perspective attributes, such as self-efficacy, security, and privacy awareness, are very critical and can represent the user's defense ability.

Moreover, perceived severity of threat was given the lowest rank in the experts' assessments, with mean only 3.4 which opposes the findings that this factor is very important in determining the individual's behaviour toward online risks [28, 49]. Both studies used self-administered questionnaires to measure the severity of threat which might be considered a common way to gauge the individual's perceived threat. Another explanation for the low rank given to perceived severity of threat has been proposed by Expert 1 as he answered that severity of threat and the likelihood of threat can be considered as a multi-attribute that provide an assessment of the user's risk perception. Likewise, Expert 4 commented that user expectation of the threats occurrence and their perception of risks associated with using social network are similar and can be combined together. The rating results show very close means between the likelihood of threat and the perceived risk which support Expert 4's comment.

Independent sample t-test

An independent samples t-test was conducted to examine whether there is a difference between the two groups in the study sample. The grouping variables used in this test are nationality and gender. Therefore, the means of the framework's items have been compared between the multi-national experts' group (first expert review phase) and Saudi experts' group (second expert review phase) to identify any impact of cultural differences on the results, and then between male and female to identify the presence of gender differences.

In order to conduct the independent samples test, two steps have been considered. First, testing the homogeneity of variance; using Levene's test for equality of variances. The hypotheses for Levene's test are: Support the null hypothesis, H0, if the Levene's test (p-value > .05), the variances of the two groups are equal (equal variances assumed). Support the alternative hypothesis, H1, if the Levene's test (p-value $\leq$ .05), the variances of the two groups are not equal (equal variances not assumed).

Second, testing means differences; as can be seen from Table 5, the output of the t-test includes two rows: equal variance assumed and equal variance not assumed. The independent samples t statistic is calculated differently in these two rows. Therefore, depending on the level of the variance from the first step the appropriate result will be read from the table. To test the means differences, alpha ($\alpha = .05$) has been chosen as Support H0 if the significance of the t-test is greater than alpha (no difference in means). Support H1 if the significance of the t-test is less than or equal alpha (there is a difference in means).

Findings and discussion

Culture comparison It can be seen from Table 5 that the Levene's test p-value for most of the items is greater than alpha (sig. > .05), which means that the null hypothesis is supported and the variances of the two groups are equal. However, one item that has rejected the null hypothesis is culture, therefore, the alternative hypothesis is supported for this item, as the variances of the two groups are not equal and indicate that the homogeneity of the variance has been violated.

Table 5 Independent samples test (culture)

	Levene's test		t-test for equality of means		Supported hypothesis		Levene's test		t-test for equality of means		Supported hypothesis
	F	Sig.	t	Sig.			F	Sig.	t	Sig.	
Per_T						Trust_M					
Equal variances assumed	2.96	.098	1.095	.284	Null	Equal variances assumed	.167	.686	− .645	.525	Null
Equal variances not assumed			1.141	.267		Equal variances not assumed			− .649	.523	
Age						Motivation					
Equal variances assumed	.181	.674	1.321	.199	Null	Equal variances assumed	.243	.626	.580	.567	Null
Equal variances not assumed			1.309	.204		Equal variances not assumed			.578	.569	
Gender						Risk					
Equal variances assumed	.345	.562	.116	.908	Null	Equal variances assumed	.542	.469	.000	1.000	Null
Equal variances not assumed			.115	.909		Equal variances not assumed			.000	1.000	
Education						Self_effic					
Equal variances assumed	2.41	.134	2.540	.018	Alternative	Equal variances assumed	.150	.702	− .643	.526	Null
Equal variances not assumed			2.432	.027		Equal variances not assumed			− .643	.527	
Comp_K						Severity					
Equal variances assumed	1.52	.229	.516	.610	Null	Equal variances assumed	.874	.359	− .690	.497	Null
Equal variances not assumed			.500	.623		Equal variances not assumed			− .681	.503	
Culture						Likelihood					
Equal variances assumed	6.41	.018	2.182	.039		Equal variances assumed	.491	.490	.324	.749	Null
Equal variances not assumed			2.077	.055	Null	Equal variances not assumed			.322	.751	
No_frind						Past_exp					
Equal variances assumed	.770	.389	.469	.644	Null	Equal variances assumed	.047	.830	.139	.891	Null
Equal variances not assumed			.460	.650		Equal variances not assumed			.138	.891	
Frq_use						Priv-Awar					
Equal variances assumed	.172	.682	− .584	.565	Null	Equal variances assumed	.282	.600	− .506	.618	Null
Equal variances not assumed			− .575	.571		Equal variances not assumed			− .515	.612	
Trust_P						Sec-Awar					
Equal variances assumed	.271	.607	− .554	.584	Null	Equal variances assumed	.174	.680	− .362	.721	Null
Equal variances not assumed			− .559	.581		Equal variances not assumed			− .366	.717	

When comparing the means in the second part of the t-test, it was clear that most of the items supported the null hypothesis (sig. > .05) as there were no differences in means between the two groups, except for one item which is education (.018).

For the education attribute, there was a difference in means between the two groups (sig. < .05). The difference of opinion here was on the importance level of the education factor, which causes the difference in means between the two groups. Yet, both groups have rated education as being on the importance side, to be included in the framework. Furthermore, there was an agreement among experts in both groups with regard to the low importance of gender differences in the user's poor judgment of social engineering based attacks in SNSs. Generally, all items in both groups were ranked on the importance side, which means that the framework's items have been confirmed by both groups of experts.

Gender comparison Since the previous section has revealed that both groups have given similar responses regarding the framework's items, this means that the data gathered from the two groups can now be combined and tested together in order to examine if the experts' gender influenced the framework's factors' validation. To this end, independent samples t-test has been conducted on two gender groups (male and female). Table 6 presents the independent samples test results.

Table 6 shows that the Levene's test p-values for most of the items are greater than alpha (sig. > .05) which means that the null hypothesis is supported and the variances of the two groups are equal, except for three items which have rejected the null hypothesis and accepted the alternative hypothesis (perceived risk, self-efficacy, and perceived severity of threat).

When comparing the means in the second step, it was clear that four items rejected the null hypothesis (the number of friends, frequency of use, perceived risk, and perceived severity of threat). For these four items, there was a difference in means between the two groups (male and female) as can be seen in Fig. 5.

According to the socio-psychological attributes, both male and female participants agree that gender is not a very important factor to predict social engineering victimization. Also, Fig. 5 indicates that there were some opposing views among the two genders with regard to habitual items and their effect on the user's vulnerability to social engineering. Male experts agreed that the number of friends and the usage frequency of a social network are not very important factors that affect the users' judgment of social engineering attacks in social network. However, female experts have the opposite opinion, as they ranked these as very important factors. Additionally, female experts are agreed about the importance of perceived risk and perceived severity of threat while, in contrast, male experts believed that perceived risk and perceived severity of threat are not very important factors to consider. Once again, these disagreements were regarding the importance level of the items while both groups ranked all items as important and should be included in the framework.

Attributes that must be added to the framework

The first and the second questions of the qualitative part of the study have been discussed earlier with the quantitative part. This section will discuss the third question

Table 6 Independent samples t-test (gender)

	Levene's test		t-test for equality of means		Supported hypothesis		Levene's test		t-test for equality of means		Supported hypothesis
	F	Sig.	t	Sig.			F	Sig.	t	Sig.	
Per_T						Trust_M					
Equal variances assumed	.002	.964	− .153	.880	Null	Equal variances assumed	1.68	.208	− 1.80	.084	Null
Equal variances not assumed			− .158	.876		Equal variances not assumed			− 2.24	.035	
Age						Motivation					
Equal variances assumed	.121	.731	.523	.606	Null	Equal variances assumed	.341	.565	− 1.59	.126	Null
Equal variances not assumed			.496	.628		Equal variances not assumed			− 1.64	.118	
Gender						Risk					
Equal variances assumed	.269	.609	− .305	.763	Null	Equal variances assumed	7.23	.013	− 1.67	.107	
Equal variances not assumed			− .305	.764		Equal variances not assumed			− 2.07	.050	Alternative
Education						Self_effic					
Equal variances assumed	.126	.725	.537	.596	Null	Equal variances assumed	6.52	.017	− 1.62	.118	
Equal variances not assumed			.551	.588		Equal variances not assumed			− 1.91	.068	Null
Comp_K						Severity					
Equal variances assumed	.185	.671	.919	.367	Null	Equal variances assumed	7.75	.010	− 1.76	.091	
Equal variances not assumed			.907	.378		Equal variances not assumed			− 2.03	.054	Alternative
Culture						Likelihood					
Equal variances assumed	.040	.843	− .153	.879	Null	Equal variances assumed	.826	.372	− .669	.510	Null
Equal variances not assumed			− .149	.883		Equal variances not assumed			− .711	.486	
No_frind						Past_exp					
Equal variances assumed	.604	.445	− 2.27	.033	Alternative	Equal variances assumed	1.70	.204	.109	.914	Null
Equal variances not assumed			− 2.56	.018		Equal variances not assumed			.122	.904	
Frq_use						Priv_awar					
Equal variances assumed	3.66	.068	− 3.36	.003	Alternative	Equal variances assumed	1.23	.278	− .714	.482	Null
Equal variances not assumed			− 4.19	.000		Equal variances not assumed			− .795	.435	
Trust_P						Sec_awar					
Equal variances assumed	3.77	.064	− 1.87	.074	Null	Equal variances assumed	1.72	.202	− .571	.573	Null
Equal variances not assumed			− 2.14	.043		Equal variances not assumed			− .671	.509	

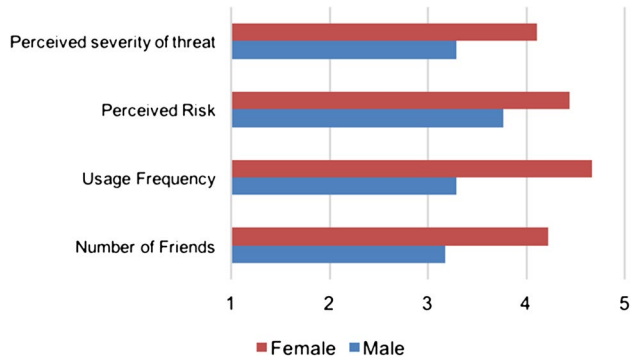

Fig. 5 Gender comparison

which asked the experts if they think there are other attributes that should be included in the framework. Expert 2 suggested adding more attributes regarding the users' knowledge of social networks, applications, and settings. In addition, Expert 7 suggested looking at the uncertainty level of the user, which might be considered under the culture factor. Expert 10 has stated, "There are many factors that can be added here but might not explain the behaviour of all social media users. However, some young people are careless and they did not deal with the social media seriously they communicate with anybody either known or not with the goal to enjoy and pass time". Expert 11 agreed with this point of view and said, "People use social media to entertain themselves and do not want to bother use them with high concentration and full attention, they usually click on any video or image without even reading the post". The suggestions from Expert 10 and Expert 11 can be categorized under the personality trait of the user and their motivation for using social media, factors that are already present in the framework.

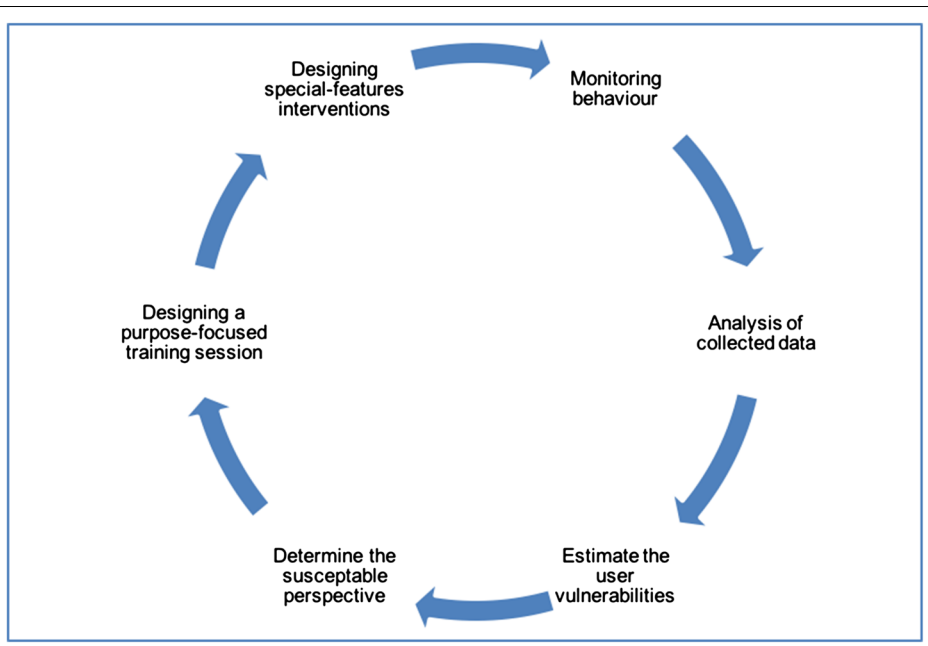

Fig. 6 A service scenario for using UCF

A service scenario for using the proposed UCF

This section introduces a potential service scenario that can enable extracting user's vulnerabilities based on our proposed model. Figure 6 presents the six steps that can identify and protect against users' vulnerabilities. Firstly, using the four proposed perspectives, the considered population's ability to deal with cyber-attacks can be tested. In this step, users' behaviour and perceptions can be collected either by monitoring or designing a questionnaire. After that, an analysis of the collected data is essential to estimate the weakest points of the considered population and to determine which perspective is considered at risk. The vulnerable perspective can be regarded as the driver for training in the subsequent step. A purpose-focused training session will be designed specifically for vulnerable users, thereby reducing the cost against training sessions for all in the considered population. Furthermore, designing interventions that could serve as a back-up for the identified weak points of vulnerable users would be useful. Finally, this process can be beneficial if conducted on a regular basis (e.g., annually). For example, if the monitoring process revealed that the population's security and privacy awareness are limited, this indicates vulnerability to exploitation in the perceptual perspective of those users. Therefore, designing a training program that focuses on increasing users' perception of the risks arising from their work environment is appropriate. The training may present real case examples on how users can maintain their knowledge and ability to secure their private data. Additionally, algorithms can be developed based on the proposed characteristics, in order to automatically identify vulnerable individuals in the population in order to provide security interventions that protect them.

Conclusion

The proposed user-centric framework was the result of integrating previous research, after conducting a comprehensive study of existing human-centric frameworks and related theories. The expert evaluation has been designed to validate the framework's attributes and the results of this validation reflect the experts' confirmation and acceptance of the framework's components. Yet, some amendments have been made to the framework according to the experts' recommendations. In the socio-psychological perspective, computer knowledge has been replaced by social network knowledge. Most social network users should already have basic computer knowledge but their knowledge of social networking sites and applications is more critical to the study purpose. In the perceptual perspective, two dimensions are included which are risk perception and the user competence dimensions. The risk perception includes the severity of threat and the likelihood of threat while user competence includes self-efficacy, privacy awareness, security awareness, and past experience. In the socio-emotional perspective, two dimensions are included which are the motivation dimension, and the trust dimension which includes the attributes of trusting SN members and trusting SN provider.

The study highlighted the riskiest factors that impact users' vulnerabilities, particularly in social network settings. Yet, how these factors interact with each other and how we can mitigate their influence is still unclear. Incorporating experts' opinion on identifying the reasons behind the failure of cyber-attack resistance is a fundamental step toward understanding why people still succumb to cyber-attacks. Detecting the prime interventions between people and the likelihood of victimisation is important for social network

providers in order to protect their users. For example, providing security and privacy tutorials that cover the four proposed perspectives would be helpful for the normal user. Classifying the users based on their habitual and socio-psychological attributes in order to identify vulnerable users is another area that network providers should consider.

The result is helpful for conducting more successful training approaches that incorporate the most important attributes from the four proposed perspectives as education elements to increase people awareness. As the identified factors might be seen as user's threats points, these factors can be targeted by enforcing behavioural security strategies to mitigate social engineering threats.

Organisations can use this framework to evaluate and understand employee perspectives when using social networks in order to initiate more effective interventions. Several types of interventions can be generated based on the present findings. Education-based interventions can be proposed to enhance people awareness and skills to detect social networks threats. Also, special-features interventions could be designed to cover up the weak points of a specific group of people. For example, if a particular company noticed a lack of privacy awareness among their employees, a tool could be designed to offer more efficient privacy control that is in keeping with the company's policy and needs.

The present study has several limitations that must be acknowledged. The experts' review approach that has been used in this study may not be considered the best way to predict user vulnerability. At some stage, this requires experimental studies, which can give more empirical and accurate results. Also, the sample size is relatively small which is often the case in expert review studies as it is difficult to find a large number of experts willing to participate in such a study. Yet, the purpose of the present study is not to generalize our proposed framework on the study area as it is the case with empirical studies but to shed light on important factors and dimensions that have not been previously addressed, especially in the context of social networks. Under this perspective, the chosen approach and the sample size used in the expert review is adequate to serve our purpose.

Another limitation is that the knowledge backgrounds of the participants are not diverse, as all of them specialise in the information security field. It would be worth knowing what experts from different disciplines think about the proposed framework. Finally, while extensive steps have been taken to ensure the inclusion of all affecting factors in the framework, it is not feasible to guarantee that all possible influences are included in this framework. Yet, this limitation has been minimised by the qualitative part of the study that includes open-ended questions. This prevented experts being limited to the framework's factors and allowed them to suggest more factors that they believed to be important. Therefore, using a mixed method approach in the expert review has eliminated the limitation of both the quantitative and the qualitative part of the study.

Future research will concentrate on empirically testing the framework factors and dimensions on the social engineering victimisation in the social network context. Also, the framework can be enhanced to suit different security issues related to cloud computing or Internet-of-Things, in order to understand the key factors affecting the individual's threat detection ability. The proposed user-centric framework could help in determining the competence level of social networks users in detecting cyber-attacks and this could provide new technical solutions that rely upon monitoring of human activities. For example, enriching security alerts by integrating network intelligence and insights upon

human behaviour. Future research can go further by automatically classifying SN users based on the framework's attributes that can be retrieved from the network in order to add an extra layer of security for those characterised as more vulnerable.

Additional file

Additional file 1. The dataset used in this study.

Abbreviations
UCF: user-centric framework; SE: social engineering; SN: social network; SNSs: social networking sites; IS: information security.

Authors' contributions
SMA conducted the experts' review, analysed the collected data, and drafted the manuscript. GRSW helped in developing a valid analysis of the experts' review and participated in drafting the manuscript. Both authors read and approved the final manuscript.

Acknowledgements
We would like to thank the experts who participated in our study for their valuable contribution.

Competing interests
The authors declare that they have no competing interests.

Ethics approval and consent to participate
This study has been approved by the University of Strathclyde Departmental Ethics Committee.

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

Appendix A

Factor	Definition
Personality traits	User behaviour can be patterned and categorised in five different traits which are: openness, conscientiousness, agreeableness, extraversion, and neuroticism
User demographics	The present study considers the importance of each demographic attribute such as age, gender, education as an independent factor
Culture	The user's nationality
Perceived risk of social network	To what extent the user is uncertain whether an online action is worthwhile or not
Experience with cybercrime	Has the individual previously faced or fallen victim for any kind of social engineering attacks such as identity theft, phishing, etc
Perceived severity of threat	The individual's perception of the severity of threats that might be occurred in social networks and the negative consequences of that threats
Perceived likelihood of threat	The individual's perception of the likelihood of threats and the possibility of falling victim to social engineering attacks in social networks
Privacy awareness	Users' attitude and actions in order to protect their personal information online
Security awareness	Users' attitude and actions that aim to protect themselves from online security threats
Self-efficacy	The individual's confidence in their ability to protect themselves against any undesirable online incidents
Level of involvement	To what extent a user engages in social network activities
Trust in provider	To what extent the individual trusts and relies on the social network's service provider to protect their personal information
Trust in members	To what extent the individual believes that other social network members are trustworthy and not harmful
Motivation to use	It is defined as the motivation that causes the individual to engage more in social networks without conducting preventive measures

Publisher's Note

Received: 31 August 2017 Accepted: 20 February 2018
Published online: 28 February 2018

References

1. Ponemon Institute and IBM Security (2017) 2017 cost of data breach study: global overview
2. Mulligan DK, Schneider FB (2011) Doctrine for cybersecurity. Daedalus 140(4):70–92
3. Martin KD, Borah A, Palmatier RW (2017) Data privacy: effects on customer and firm performance. J Mark 81(1):36–58
4. Hinz O, Nofer M, Schiereck D, Trillig J (2015) The influence of data theft on the share prices and systematic risk of consumer electronics companies. Inf Mana 52(3):337–347
5. Weiss NE, Miller RS (2015) The target and other financial data breaches: frequently asked questions. Congr Res Serv 4:1–38
6. Singh MM, Ng PJ, Yap KM, Husin MH, Malim NHAH (2017) Cyberbullying and a mobile game app? An initial perspective on an alternative solution. J Inf Process Syst 13(3):559–572
7. Vishwanath A (2015) Habitual Facebook use and its impact on getting deceived on social media. J Comput Commun 20(1):83–98
8. Irani D, Balduzzi M, Balzarotti D, Kirda E and Pu C (2011) Reverse social engineering attacks in online social networks. In: International conference on detection of intrusions and malware, and vulnerability assessment. pp 55–74
9. Shindarev N, Bagretsov G, Abramov M, Tulupyeva T and Suvorova A (2018) Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities. In: Abraham A, Kovalev S, Tarassov V, Snasel V, Vasileva M, and Sukhanov A (eds) Proceedings of the second international scientific conference "Intelligent Information Technologies for Industry" (IITI'17): volume 1. Springer International Publishing, pp 441–447
10. Edwards M, Larson R, Green B, Rashid A, Baron A (2017) Panning for gold: automatically analysing online social engineering attack surfaces. Comput Secur 69:18–34
11. Polakis I, Kontaxis G, and Antonatos S (2010) Using social networks to harvest email addresses. In: Proceedings of the 9th annual ACM workshop on privacy in the electronic society. pp 11–20
12. Iuga C, Nurse JRC, Erola A (2016) Baiting the hook: factors impacting susceptibility to phishing attacks. Human Centric Comput Inf Sci 6(1):8
13. Darwish A, El Zarka A, and Aloul F (2012) Towards understanding phishing victims' profile. In: 2012 international conference on computer systems and industrial informatics (ICCSII 2012). pp 13–17
14. Uebelacker S and Quiel S (2014) The social engineering personality framework. In: 2014 workshop on socio-technical aspects in security and trust. IEEE, New York, pp 24–30
15. Mohebzada J, El Zarka A, Bhojani A, and Darwish A (2012) Phishing in a University Community. In: International conference on innovations in information technology (IIT). pp 249–254
16. Williams EJ, Beardmore A, Joinson AN (2017) Individual differences in susceptibility to online influence: a theoretical review. Comput Hum Behav 72:412–421
17. Krombholz K, Hobel H, Huber M, Weippl E (2015) Advanced social engineering attacks. J Inf Secur Appl 22:113–122
18. Foozy C, Ahmad R, and Abdollah M (2011) Generic taxonomy of social engineering attack. In: Malaysian technical universities international conference on engineering technology MUiCET (2011), MUiCET. pp 527–533
19. Rathore S, Sharma PK, Park JH (2017) XSSClassifier: an efficient XSS attack detection approach based on machine learning classifier on SNSs. J Inf Process Syst 13(4):1014–1028
20. Algarni A, Xu Y, Chan T, and Tian Y (2013) Social engineering in social networking sites : affect-based model. In: The 8th IEEE international conference for internet technology and secured transactions (ICITST-2013). pp 508–515
21. Bertino E and Ferrari E (2018) Big data security and privacy. In: A comprehensive guide through the Italian database research over the last 25 years, vol 31. Springer International Publishing, Berlin, pp 425–439
22. Vishwanath A, Harrison B, Ng YJ (2016) Suspicion, cognition, and automaticity model of phishing susceptibility. Commun Res 1–21. https://doi.org/10.1177/0093650215627483
23. Halevi T, Lewis J, and Memon N (2013) Phishing, personality traits and Facebook. arXiv Prepr. arXiv1301.7643
24. Vishwanath A, Herath T, Chen R, Wang J, Rao HR (2011) Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decis Support Syst 51(3):576–586
25. Sherchan W, Nepal S, Paris C (2013) A survey of trust in social networks. ACM Comput Surv 45(4):47
26. Saridakis G, Benson V, Ezingeard JN, Tennakoon H (2016) Individual information security, user behaviour and cyber victimisation: an empirical study of social networking users. Technol Forecast Soc Change 102:320–330
27. M. Al-Qurishi, M. Alrubaian, S. M. M. Rahman, A. Alamri, and M. M. Hassan, "A prediction system of Sybil attack in social network using deep-regression model," *Futur. Gener. Comput. Syst.*, 2017
28. Workman M, Bommer WH, Straub D (2008) Security lapses and the omission of information security measures: a threat control model and empirical test. Comput Hum Behav 24(6):2799–2816
29. Vance A, Siponen M, Pahnila S (2012) Motivating IS security compliance: insights from habit and protection motivation theory. Inf Manag 49(3–4):190–198
30. 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
31. 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
32. Islam MB, Watson J, Iannella R, Geva S (2017) A greater understanding of social networks privacy requirements: the user perspective. J Inf Secur Appl 33:30–44

33. Alseadoon I, Othman MFI, and Chan T (2015) What is the influence of users' characteristics on their ability to detect phishing emails? In: Advanced computer and communication engineering technology. Springer International Publishing, Berlin, pp 949–962
34. Sheng S, Holbrook M, Kumaraguru P, Cranor LF, and Downs J (2010) Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the 28th international conference on human factors in computing systems-CHI'10. pp 373–382
35. Al-Hamar M, Dawson R, and Guan L (2010) A culture of trust threatens security and privacy in Qatar. In: 10th IEEE international conference on computer and information technology (CIT-2010). pp 991–995
36. 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
37. Workman M (2008) Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. J Am Soc Inf Sci Technol 59(4):662–674
38. 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
39. Cheung-Blunden V, Ju J (2016) Anxiety as a barrier to information processing in the event of a cyberattack. Political Psychol 37(3):387–400
40. Farrahi K, Zia K (2017) Trust reality-mining: evidencing the role of friendship for trust diffusion. Human Centric Comput Inf Sci 7(1):4
41. Dwyer C, Hiltz SR, and Passerini K (2007) Trust and privacy concern within social networking sites : a comparison of Facebook and MySpace. In: Proceedings of americas conference on information systems (AMCIS). pp 339
42. Albladi S, and Weir GRS (2016) Vulnerability to social engineering in social networks : a proposed user-centric framework. In: International conference on cybercrime and computer forensics (ICCCF 2016)
43. Parrish JL Jr, Bailey JL, and Courtney JF (2009) A personality based model for determining susceptibility to phishing attacks. In: Southwest Decision Sciences Institute (SWDSI) annual meeting, July 2015. pp 285–296
44. Benson V, Saridakis G, Tennakoon H (2015) Purpose of social networking use and victimisation: are there any differences between university students and those not in HE? Comput Hum Behav 51:867–872
45. Aguti B, Wills GB, and Walters RJ (2015) An evaluation of the factors that impact on the effectiveness of blended e-learning within universities. In: International conference on information society, i-society 2014. pp 117–121
46. Yahya F, Walters RJ, and Wills GB (2016) Goal-based security components for cloud storage security framework: a preliminary study. In: International conference on cyber security and protection of digital services, cyber security 2016. pp 1–5
47. De Winter JCF, Dodou D (2010) Five-point Likert items: t test versus Mann–Whitney–Wilcoxon. Pract Assess Res Eval 15(11):1–12
48. Norman G (2010) Likert scales, levels of measurement and the "laws" of statistics. Adv Heal Sci Educ 15(5):625–632
49. Alqarni Z, Algarni A, and Xu Y (2016) Toward predicting susceptibility to phishing victimization on Facebook. In: IEEE international conference on services computing. pp 419–426