Factors Affecting Users' Judgment of Cyberattacks

Samar Muslah Albladi[1]; George Weir[2]
University of Strathclyde, Department of Computer & Information Sciences

Abstract

The number of social engineering attacks has risen dramatically in the past few years, causing unpleasant damage both to organizations and to individuals. Yet, little research has discussed social engineering in the virtual environments of social networks (SN). Moreover, there were no agreement regarding the user's characteristics that may make the user more vulnerable to social engineering in social networks. Therefore, The present study proposes a user-centric framework to identify the factors that most impair users judgment of cyberattacks based on four perspectives: Socio-psychological, Habitual, Socio-emotional, and Perceptual as previous research has mainly focused on Socio-psychological perspective while other important perspectives remain relatively unexplored. A mixed method approach has been adopted to validate the framework factors and components.

Introduction and Aims

Research has repeatedly identified the human as the weakest link in information security. The factors that influence the user's judgment of social engineering based attacks in social networking must be investigated [1]. The present research aims to identify the user characteristics, dimensions and variables that influence such user judgments and provide a new theoretical framework to understand users' behaviour toward social network deception. The proposed user-centric framework **(Figure 1)** was based on the integration of previous literature and relevant theories [1].

User Characteristics			
Socio-psychological	**Perceptual**	**Habitual**	**Socio-Emotional**
a. Personality trait b. User demographic: age, gender, education, computer knowledge c. Culture	a. Perceived risk of social network b. Past experience with Social engineering c. Perceived severity of Threat d. Perceived likelihood of Threat e. Privacy awareness f. Security awareness g. Self-efficacy	a. The level of engagement: • Number of friends • Frequency of use	a. Trusting social network provider b. Trusting social network members c. Motivation to use
Vulnerability Level: High or Low			

Figure 1. The proposed User-Centric Framework (UCF) [1]

Methods

- A mixed method experts review has been used as an approach to validate the proposed framework dimensions and components. **Figure 2** summarises the validation process.
- Two rounds of experts review have been conducted on two groups (first group→14 participants, second group →12).
- Participants were presented with a short questionnaire asking them to rate the importance of each factor to the study context and then express their comments and suggestions by answering 3 open-ended questions:
  - 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?

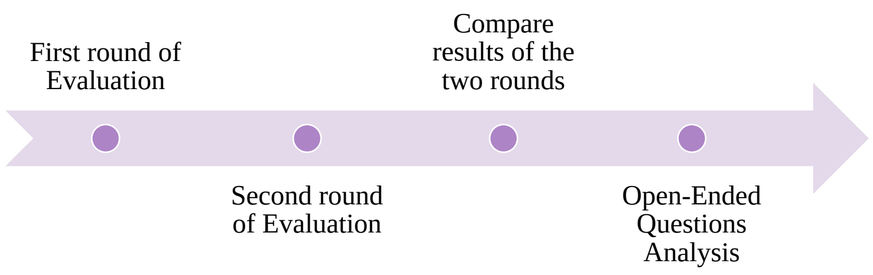
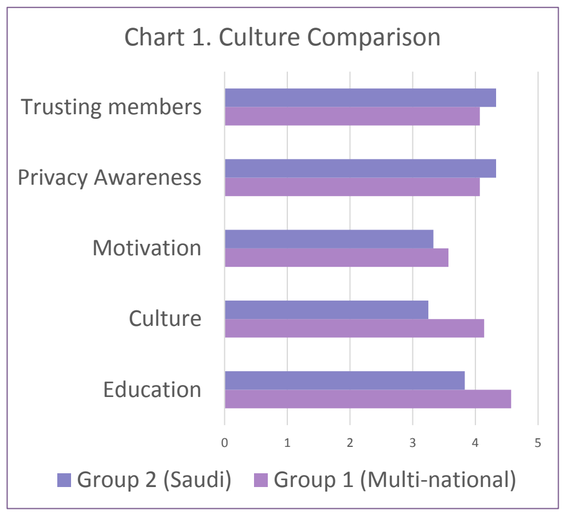
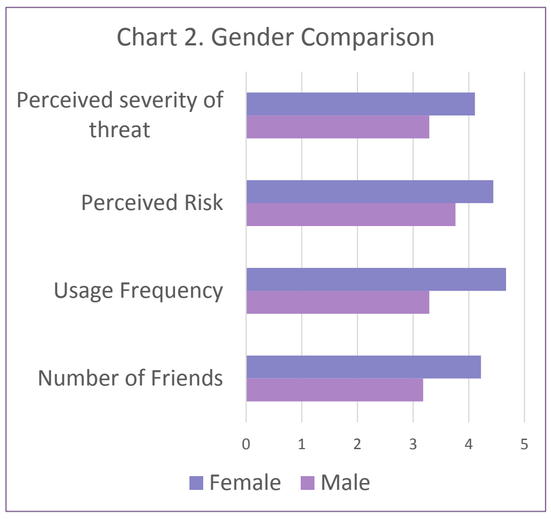


Figure 2. UCF validation process

Quantitative Results

- An independent t-test was conducted to examine whether there is a difference between the two groups in the study sample.
- The grouping variables (Nationality, Gender).
- The means of the Framework's items have been compared between the multi-national Experts' group (first expert review round) and Saudi Experts' group (second expert review round) to identify any impact from **cultural differences (Chart 1)** on the results, and then between male and female to identify the presence of **gender differences (Chart 2).**





Qualitative Results

- Some amendments have been made to the framework according to the experts' recommendations.
- In the **socio-psychological perspective**,
  - Computer knowledge → Social network knowledge.
- In the **perceptual perspective**,
  - Risk perception dimension: the severity of threat and the likelihood of threat.
  - User competence dimension: self-efficacy, privacy awareness, security awareness, and past experience.
- In the **socio-emotional perspective**,
  - Motivation dimension
  - Trust dimension: trusting SN members and trusting SN provider.

User Characteristics			
Socio-psychological	**Perceptual**	**Habitual**	**Socio-Emotional**
a. Personality trait **b. User demographic**: age, gender, education **c. Culture**	**a. Risk Perception** • Perceived Severity of threat • Perceived likelihood of threat **b. User Competence** • Self-efficacy • Privacy awareness • Security awareness • Past experience	**a. The level of Engagement**: • Number of friends • Frequency of usage • Time since having a SN account	**a. Trust** • Trusting social network provider • Trusting social network members **b. Motivation to use**
Vulnerability Level: High or Low			

Figure 3. The validated UCF

Conclusion

- ✓ There was significant agreement among experts in regards to the importance of the framework's factors which reflected their confirmation and acceptance of the framework components.
- ✓ Technology defensive techniques usually assume no differences between online users while in fact, users can be classified according to their weakness in detecting online threats. This classification will help assign the right defensive technique or training for potential victims.
- ✓ Future research will focus on empirically examining the proposed framework constructs and their impact on social engineering victimization.

Contact
[1] samar.albladi@strath.ac.uk
[2] george.weir@strath.ac.uk

References
1. S. Albladi and G. R. S. Weir, "Vulnerability to Social Engineering in Social Networks : A Proposed User-Centric Framework," in *International Conference on Cybercrime and Computer Forensics (ICCCF 2016)*, 2016.