A Conceptual Model to Predict Social Engineering Victims

Samar Muslah Albladi[1], George R S Weir
Department of Computer and Information Sciences
University of Strathclyde, UK
[1]samar.albladi@strath.ac.uk

12th International conference on Global Security, Safety and Sustainability (ICGS3-19)

1. Introduction

Social engineering (SE) attacks are a serious threat to online users and might subject people to different kinds of harm. 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. The number of victims of social engineering attacks will be decreased if the users' detection ability has improved. Yet, this improvement of the user's detection behaviour can't be occurred without investigating the users' weakness points. The present study develops a conceptual model to test the factors that influence social networks users' judgment of social engineering-based attacks in order to identify the weakest points of users' detection behaviour which also help to predict vulnerable individuals.

2. Motivation and Background

Security practitioners still relying 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 (2018), the number of using social engineering attacks to exploit human vulnerabilities has dramatically increased over the last year. This arises the necessity of finding a solution that helps the user to show acceptable defensive behaviour in the social network (SN) reality. Identifying the user characteristics that make them more or less vulnerable to social engineering threats is vital to protect against such threats. Identifying the weakest points can help users to recognise their perceptual and habitual limits and to target these limitations by a personalised advisory system that could be designed to fit the user needs which could provide new insights to social engineering mitigation solutions.

3. Major Contributions

- Proposing a conceptual model that includes varieties of user-related factors such as socio-psychological, habitual, perceptual, and socio-emotional. 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 based on different perspectives of human-related factors.
- Proposing a new influencing perspective, socio-emotional, that hasn't been satisfactory reported in the literature.
- The current research aims to gain insight into user competence in detecting security threats in the context of online social networks and investigates the multidimensional space that determines this user competence level.

4. Methodology

➢ Participants were presented with an online-questionnaire which incorporated three main parts:

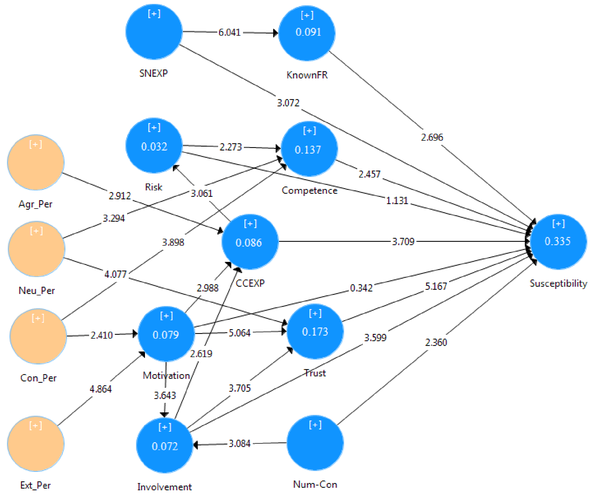
- Demographic questions.
- Questions that measure the constructs of the proposed model.
- The scenario-based experiment which includes 6 images of Facebook posts (4 high-risk scenarios, and 2 low-risk scenarios). Each post contains a type of cyber-attack such as phishing, clickjacking, malware, phishing scam. Participants were asked to indicate their response to these attacks if they encounter them in their real accounts by answering number of questions.

➢ 316 participants have completed the study questionnaire. Participants' demographics include a variety of profiles in terms of gender (39% male, 61% female), education level, and major. However, the majority (76%) of participants were younger adults (age 18-24).

5. Experimental Design

To evaluate the proposed model, partial least squares structural equation modelling (PLS-SEM) has been used due to its suitability of dealing with complex predictive models. SmartPLS v3 software package was used to analyse the model.

6. Results



Hypo	Relationship	Total effect	T-value	P-value	95% Confidence interval		Sig.?
Ha1	Involvement -> Susceptibility	0.315	5.067	0.000	0.191	0.436	Yes
Ha2	Num-Con -> Susceptibility	-0.038	0.841	0.401	-0.125	0.051	No
Ha3	KnownFR -> Susceptibility	-0.127	2.696	0.007	-0.217	-0.033	Yes
Ha4	SNEXP -> Susceptibility	-0.201	4.090	0.000	-0.296	-0.100	Yes
Ha5	Risk -> Susceptibility	-0.077	1.518	0.129	-0.177	0.023	No
Ha6	Competence -> Susceptibility	-0.125	2.457	0.014	-0.222	-0.025	Yes
Ha7	CCEXP -> Susceptibility	0.208	3.521	0.000	0.088	0.322	Yes
Ha8	Trust -> Susceptibility	0.286	5.167	0.000	0.179	0.398	Yes
Ha9	Motivation -> Susceptibility	0.180	3.908	0.000	0.088	0.268	Yes

Num-Con: number of connections, **KnownFR:** percentage of known friends, **SNEXP:** social network experience, **CCEXP:** cybercrime experience

7. Discussion

- The findings of this research indicate that most of the considered user characteristics factors influence users' vulnerability either directly or indirectly.
- People trust in the social network's provider, and members were the strongest determinant of their vulnerability to SE attacks. This support our claims that socio-emotional factors are fundamental to consider.
- The individual competence level to deal with cybercrime, which was measured based upon three dimensions, i.e., security awareness, privacy awareness, and self-efficacy, found to significantly predict the individual's ability to detect SE attacks on Facebook.
- The present study found personality traits (except openness to experience) to be significant predictors of human vulnerability to cyber-attacks. Yet, these relations are indirect and mediated by other relevant factors.

8. Conclusions

The present study provides evidence that individuals' characteristics can predict vulnerable people to SE victimisation and their effects should be considered in future studies when designing training and awareness programs.

9. Future Work

- This study on determining user vulnerabilities affords a basis for profiling users according to their characteristics and weakness in respect of particular threats.
- In turn, this provides a means for future studies to design a personalised advisory system that sends awareness posts to target individual user needs.