2014

SOCIAL ENGINEERING IN SOCIAL NETWORKING SITES: HOW GOOD BECOMES EVIL

Abdullah Algarni
School of Electrical Engineering and Computer Science, Queensland University of Technology, abdullahayedm.algarni@student.qut.edu.au

Yue Xu
School of Electrical Engineering and Computer Science, Queensland University of Technology, yue.xu@qut.edu.au

Taizan Chan
School of Electrical Engineering and Computer Science, Queensland University of Technology, t.chan@qut.edu.au

Yu-Chu Tian
School of Electrical Engineering and Computer Science, Queensland University of Technology, y.tian@qut.edu.au

SOCIAL ENGINEERING IN SOCIAL NETWORKING SITES: HOW GOOD BECOMES EVIL

Abdullah Algarni, School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane, Australia, abdullahayedm.algarni@student.qut.edu.au

Yue Xu, School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane, Australia, yue.xu@qut.edu.au

Taizan Chan, School of Information Systems, Queensland University of Technology, Brisbane, Australia, t.chan@qut.edu.au

Yu-Chu Tian, School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane, Australia, y.tian@qut.edu.au

Abstract

Social Engineering (ES) is now considered the great security threat to people and organizations. Ever since the existence of human beings, fraudulent and deceptive people have used social engineering tricks and tactics to trick victims into obeying them. There are a number of social engineering techniques that are used in information technology to compromise security defences and attack people or organizations such as phishing, identity theft, spamming, impersonation, and spaying. Recently, researchers have suggested that social networking sites (SNSs) are the most common source and best breeding grounds for exploiting the vulnerabilities of people and launching a variety of social engineering based attacks. However, the literature shows a lack of information about what types of social engineering threats exist on SNSs. This study is part of a project that attempts to predict a persons' vulnerability to SE based on demographic factors. In this paper, we demonstrate the different types of social engineering based attacks that exist on SNSs, the purposes of these attacks, reasons why people fell (or did not fall) for these attacks, based on users' opinions. A qualitative questionnaire-based survey was conducted to collect and analyse people's experiences with social engineering tricks, deceptions, or attacks on SNSs.

Keywords: Social engineering, social networking sites, deception; privacy, trust, information security management.

1 INTRODUCTION

Social networking sites (SNSs) are great places for people to communicate with each other and share knowledge. Many companies have adapted SNSs to promote collaboration among employees, communicate with customers, and advertise products and services. However, SNSs are also ideal places for social engineering based attacks and threats. As the number of SNSs users has been increasing dramatically, the amount of sensitive and private information of people, companies, organizations, or governmental institutions and their activities is also increasing dramatically. This not only makes SNSs attractive to faithful users but also makes them perfect breeding grounds for malicious users and attackers. Information is always under threat, and it can be intercepted, modified, or exposed. The facilities that are setup to monitor such attacks are also constantly under attack (Zhang et al. 2010). Such attacks shape the challenges of providing usability and sociability, which are the main purposes of SNSs, as well as ensuring integrity, confidentiality, and availability, which are standard principles of security.

Deceiving or influencing people to provide critical information or to perform an action that will benefit the attacker is known as "social engineering" (Mitnick et al. 2001). Fraudulent and deceptive people have been using social engineering traps and tactics using social networking sites to trick victims into obeying them, accepting threats, and falling victim to various crimes and attacks such as phishing, sexual abuse, financial abuse, identity theft, impersonation, physical crime, and many other forms of attack. Several studies have investigated and highlighted the risks associated with social engineering in SNSs, e.g., (Dimensional-Research 2011); (Hogben 2007); (Nagy et al. 2009); (Jagatic et al. 2007); (Algarni et al. 2013); and (Chitrey et al. 2012). Those studies suggest that SNSs are among the most common source of social engineering threats. Although these studies and many others show the risk associated with social engineering in SNSs, more research needs to be done to address such threat. This study is part of a project that attempts to predict a person's vulnerability to SE based on demographic factors (e.g., age, gender, and educational level), relationship status, and personality type. It is a part of a project that uses a *sequential exploratory mixed method*, starting with a qualitative phase followed by a quantitative phase. In this present study, a qualitative questionnaire-based survey was used to anonymously investigate peoples' real experience in terms of social engineering based attacks in SNSs, and therefore to encourage participants to report their real experience without hesitation so that we gain as much knowledge as possible about the phenomenon.

2 LITERATURE REVIEW AND RELATED WORK

The strong relationship between deception and social engineering illustrates the complexity of detecting and controlling social engineering based attacks (Algarni et al. 2013b). On the organizational level, the findings of a study done by Kvedar (2010), suggest that social engineers could succeed even among those organizations that identify themselves as being aware of social engineering techniques (Kvedar et al. 2010). Marett et al. (2004) have explained that the reason why people are weak and perform poorly in detecting deception is because of the "lie detector bias," which is the assumption that most people are telling the truth (Marett et al. 2004). Most of the books and studies that have been published regarding social engineering indicate that the main causes of human weaknesses that lead people to fall victim to social engineers are human sociopsychological characteristics (Bezuidenhout et al. 2010; Mohebzada et al. 2010; Pattinson et al. 2012; Twitchell 2006). Human sociopsychology has been discussed in relation to social engineering to understand why humans are the weakest link in information security (Bezuidenhout et al. 2010; Gragg 2003; Mitnick et al. 2001; Nohlberg 2008; Peltier 2006). However, the discussions in these studies are mainly focused on persuasion and influence in marketing, especially the principles of influence outlined by Cialdini (Cialdini 2001). Cialdini suggests that liking, reciprocity, scarcity, social proof, fear, and strong affect are the main tools of persuading customers in order to buy certain products or services. Although the extant literature considers the principles of persuasion and influence on the basis of marketing as human vulnerabilities, that literature revealed no theoretical framework specifically grounding the study of the factors affect social engineering threats in information security.

The common techniques of social engineering that are suggested in the current literature include the following: "Phishing," which is enticing a victim to download an attachment or to click on an embedded hyperlink or tricking the victim to reveal critical information such as username and password (Coronges et al. 2012); "persuasion and bribery," which is attempting to persuade an employee to do an action even if this action bypasses company rules (Richardson 2007); "shoulder surfing," which involves looking over an unsuspecting user's shoulder while he/she is entering his/her user name and password or while he/she is doing his/her work; "spam," which involves sending messages to various people to ask for certain personal information, to get them to buy or sell products and services, or to ask them to participate or donate for charitable works (Mohebzada et al. 2010); "dumpster diving," which is looking for valuable information in a company dumpster to find a phone directory, for example (Richardson 2007); "reverse attack," in which the attacker does not establish contact with the victim, but rather, the social engineer tricks victims into contacting him/her. In the reverse attack case, the victim will be extremely trusting of the attacker, and the attacker will take the chance to ask the victim to give up any information or to do any action (Irani et al. 2011). While some of those techniques are presented in the literature based on real life situation or using email messages, the same techniques can be done in SNSs easily by spying on the users' activities and posts, or by diving into users' profiles, groups, events, and pages to look for any valuable information that can help attackers to trick users directly or indirectly (Algarni et al. 2013a).

The commonly suggested countermeasures for defending against social engineering based attacks include the following: "Education and training" which involves developing security awareness and training programs to train employees in ways to resist social engineering (Brody 2012). "Policy and management" which involves developing clear and concise security protocols that are enforced consistently throughout the organization, as well as developing simple rules defining what information is sensitive (Gragg 2003; Kvedar et al. 2010); "Auditing and testing" which involves testing employees' susceptibility to social engineering based attacks (Mitnick et al. 2001). The literature shows that there is a severe lack of research dedicated to the susceptibility of social engineering victimization in SNSs, or to understanding which demographic factors correlate with falling for social engineering tricks in SNSs. However, there are a few studies that have the measured susceptibility to specific types of phishing email attacks (which is a type of social engineering based attacks) or studied the effectiveness of one or more phishing countermeasures in relation to some demographic factors, e.g., (Jagatic et al. 2007), (Kvedar et al. 2010), (Pattinson et al. 2012), (Workman 2008), (Kumaraguru et al. 2009), (Parrish Jr et al. 2009), (Sheng et al. 2010), and (Darwish et al. 2012). The difference between our study and those studies is that our focus is social engineering in SNSs and not on using e-mail. Moreover, we are interested in investigating the factors that influence users to fall victims for social engineering in SNSs and if there is a relationship between the affectedness of each factor and user demographics or personality type.

3 RESEARCH METHOD

3.1 Objective

The qualitative questionnaire-based survey is a technique whereby the researcher gains a deep understanding of the human behaviors as well as the different reasons that govern their behaviors (Denzin et al. 2005). A qualitative method is one that engages in the investigations with regard to the how and the why of the decision making rather than just focusing on when, where, and what questions. Thus, a small sample-size can be sufficient if saturation is reached, and statistical confidence is not needed to be computed (Creswell et al. 2007). Saturation is the point when the researcher is no longer seeing of finding new factors, which occurs in this study in the first forty participations. Because of the sensitivity surrounding the subject, and to encourage more participants, we made the survey concise and the participation anonymous. Moreover, to avoid fabricated stories or bias, we made the participation totally voluntary. A pilot study was conducted, first to test the reliability of the questionnaire and to examine which questions needed revision. Definitions, explanations, and examples were given at the beginning of the survey to illustrate what we mean by social engineering

based attacks, social networking sites, and the purpose of the study. Demographic variables were also provided as a drop-down list to choose from, and the following specific questions were asked:

1) Have you experienced, faced, or run across any social engineering based attack in SNSs, such as deception, abuse, damage, loss, fraud, or any other type of social engineering based attacks?
2) What type of social engineering based attacks have you run across? Please tell us your experience.
3) In which social networking sites did this happened?
4) How did you respond to it?
5) Why did you respond to it in this way?

3.2 Sampling and Approaching

A letter of invitation for participation was sent to various organizations asking the directors if they would be willing to disseminate it to their personnel. Two organizations accepted the request and disseminate the invitation to their personal. More than four thousand people have been approached, a total of 78 responses were collected, and their participation was voluntary. The sample that was approached includes both genders (male and female), a variety of ages (from 18 to 60 years), and a variety of education levels (secondary school, bachelors, masters, and PhD). Moreover, the respondents are random people, represent diversity in demographics as we will describe in the findings section, and have at least one account in SNSs.

3.3 Data Analysis

A total of 78 responses were collected. However, after critical screening, six responses were not relevant to social engineering based attacks and were therefore discarded. Thematic analysis—a technique whereby the researcher identifies themes or patterns in the data thought to reflect the participants' experiences—was then used to analyze the data (Braun et al. 2006). The researcher begins with "open coding" to find core categories. In this study, the core categories are the main dimensions of the factors influencing the users' judgment of source credibility. After identifying the major factors, the researcher starts "axial coding," which seeks to find categories under each core category. Axial coding involves finding causal conditions (which determine what factor causes what effect), strategies (which are actions taken in response to the core problem), and consequences (which are the effects of using the strategies) (Corbin et al. 1990; Strauss et al. 1998). Finally, the researcher performs "selective coding," which seeks to develop link and relationship that are interrelated with the categories.

4 FINDINGS

4.1 Purposes of Social Engineering Based Attacks in SNSs

Although SNSs are basically web-based applications, and the current literature review has focused on finance-based purposes and attacks, the questionnaire results show that attackers and deceivers use social engineering tricks and techniques for a variety of reasons and purposes. As represented in Figure 1, approximately 21 percent of the participants stated that they have run across an actual or attempted sexual-purpose attack (any involuntary sexual act in which a person is threatened, or manipulated to engage against their will); 44 percent have run across an actual or attempted of financial-purpose attack (forcing, manipulating, or tricking the user to make action that will benefit the attacker financially) ; 6 percent have run across an actual or attempted reputation-destruction-purpose attack (reputation destruction of product, person, or company); 1 percent have run across an actual or attempted sport-fanaticism-purpose attack; 6 percent have run across an actual or attempted political-purpose attack; 3 percent have run across an actual or attempted religion-or-belief-purpose attack (Approving a specific belief or attacking another belief); 4 percent have run across an actual or attempted increasing the number of friends-purpose (prestige-purpose) attack; 4 percent have run across an actual or attempted pleasure-purpose attack and 11 percent have run across an actual or attempted unclear or unknown-purpose attack.

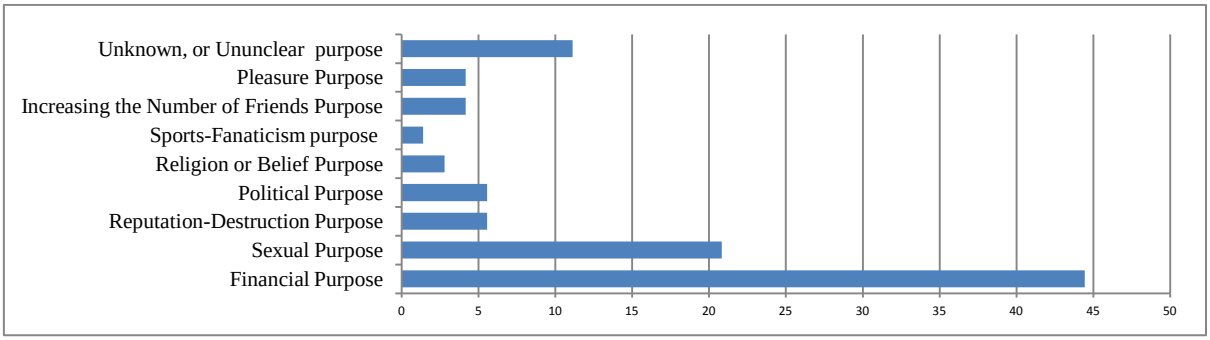

Figure 1. Percentages of Purposes of SE Based Attacks in SNSs

4.2 Techniques and Types of Social Engineering Based Attacks

To reiterate, while a review of the current literature suggests the following common techniques and types of social engineering based attacks: e-mail phishing, persuasion and bribery, shoulder surfing, e-mail spam, dumpster diving, and reverse attack, the questionnaire results of our study show how some of these techniques can be performed in SNSs, and show also some additional techniques and types of social engineering that are being used in SNSs. These types or techniques are:

- Identity theft, such as making profiles using the identities of others.
- Fake credentials, such as making fake pages of companies or organizations and supporting those fake pages with fake logos and information.
- Impersonation, such as playing the role of a sexy girl, a poor person, a company page, a famous actor, a doctor, or a businessperson.
- Copyright violation, such as stealing photos or posts.
- Content-based phishing, such as posts or news that offer jobs or services and ask for critical information in order to win or obtain that offer.
- Application-based phishing, such as games that acquires access to private information or other types of harmful applications.
- Interpersonal deception, such as friendship that ends with emotional, sexual, or financial abuse.
- Dishonest and malicious contents, such as fake stories, videos, photos, or other types of posts that aim to destroy or increase the reputation of a person, product, or party.

These new findings have emerged perhaps because this paper is among the first few papers to investigate social engineering in SNSs, which have specific and different characteristics than using e-mails, telephone, or face-to-face social engineering. Figure 2 shows the questionnaire results regarding the techniques and types of social engineering based attacks. It is important to mention here that some reported incidents include more than one type of technique.

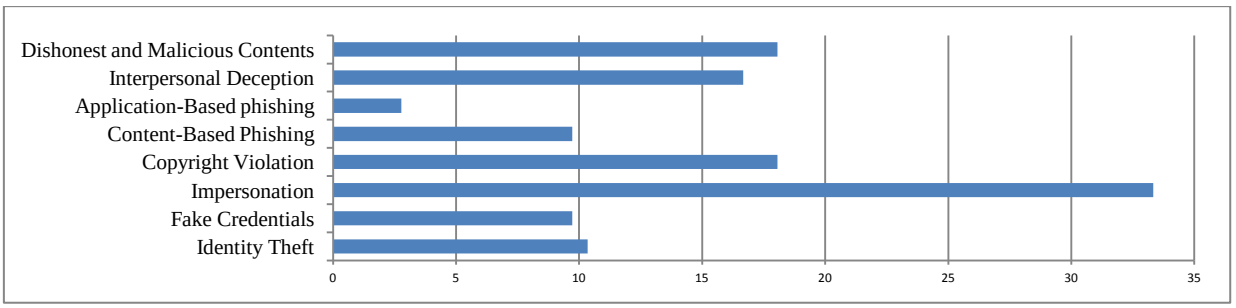

Figure 2. Percentages of Techniques and Types of SE Based Attacks

4.3 Types of Responses to These Attacks

The questionnaire results point out a very important issue in regard to social engineering based attacks in SNSs. That is, in e-mail-, telephone-, or face-to-face-based social engineering, the reaction of the

targeted victim is usually either falling for the attack or rejecting it. However, the questionnaire results show that the users of SNSs can participate in distributing tricks and attacks even if they did not fall to these attacks. Some of the participants of this survey admitted that they have participated in distributing tricks or attacks using some features of SNSs such as "liking," "retweeting," or "sharing." As shown in figure 3, there are three types of responses reported by the participants in this study who had run across any type of social engineering trick or attack:
Type 1: Discovering the deception or the trick and rejecting it.
Type 2: Accepting, or falling for a social engineering trick or attack.
Type 3: Accepting, or falling for a social engineering trick and participating in distributing it.

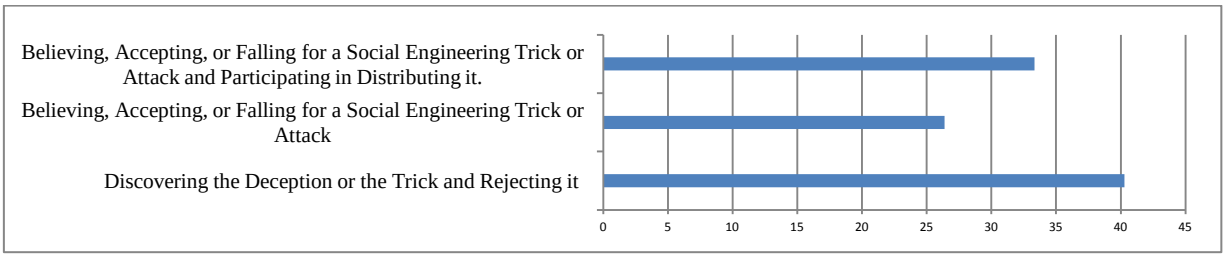

Figure 3. Percentages of the Types of Responses to SE Attacks

4.4 The SNSs through which Participants Encountered Tricks

Figure 4 shows the different SNSs that participants identified as the places that their reported stories of social engineering based attacks took place. However, it is important to mention here that some participants did not indicate the specific SNS or they indicated more than one SNS.

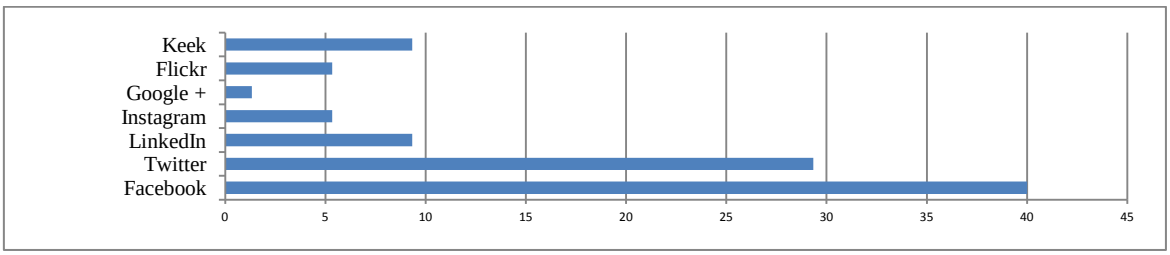

Figure 4. Percentages of SNSs through which Participants Encountered SE

4.5 Common Reasons Why Participants Fell for Social Engineering Tricks

The current literature review suggests that the main causes or reasons people fall for social engineering based attacks are the human sociopsychological factors. Our questionnaire results analysis also agreed that human sociopsychological factors are the main reasons people fall vatic to such attacks. However, we think that our questionnaire results show a better picture of how these sociopsychological factors influence people to fall for social engineering tricks, because the participants were asked "Why did you respond to the attack or the attempt of attack in this way?" They answered, as shown in figure 5, by one or more of the following answers:

- Wanting to help, such as helping an attacker who played the role of poor person or representative of a charitable organization asking for donations.
- Falling in love or into an emotional or sexual relationship, such as obeying or revealing personal information to an attacker who acted the part of a sexy girl or handsome guy.
- Feeling too shy to say *no*.
- Wanting to try, see, or accept something offered by an attacker, such as downloading "harmful" applications, videos, or photos.
- Developing trust through a long-term relationship with an attacker, which the attacker then exploits to attack the victim.
- Feeling safe from or unaware of threat because of phony webpages, logos, and contents that deliver a trick or harmful offer.

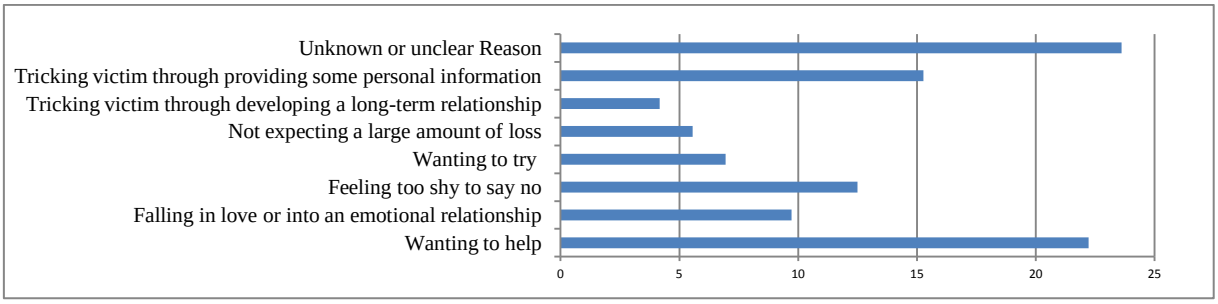

Figure 5. Percentages of Common Reasons Why Participants Fell for SE Tricks

4.6 Common Causes for Participation in Distributing Social Engineering Tricks

Our questionnaire results show that human sociopsychological factors can be also the main reasons why people participate in distributing social engineering tricks. However, although our questionnaire results show some common sociopsychological factors in both falling for tricks and participating in distributing them, among other users, the results also show different sociopsychological reasons behind why people participate in distributing social engineering tricks in SNSs, even if they did not fall victim to them (As shown in figure 6):

- Wanting to help, such as helping friends or users who might be in need of something offered by an attacker by "sharing", "liking", or "retweeting" the attacker's offer. This offer may be a job, prize, or deal that requires victims to provide personal information.
- Approving a specific belief in a post with an embedded attack that activates emotional religious, political, or other feelings, leading users to "share", "like", or "retweet" the malicious content.
- Wanting to impress or amaze others by "sharing", "liking", or "retweeting" an amazing story or post with an embedded attack or trick.
- Seeking prestige or acceptance by "sharing", "liking", or "retweeting" something offered by an attacker that requires victims to provide information or perform a harmful act to obtain the offer.

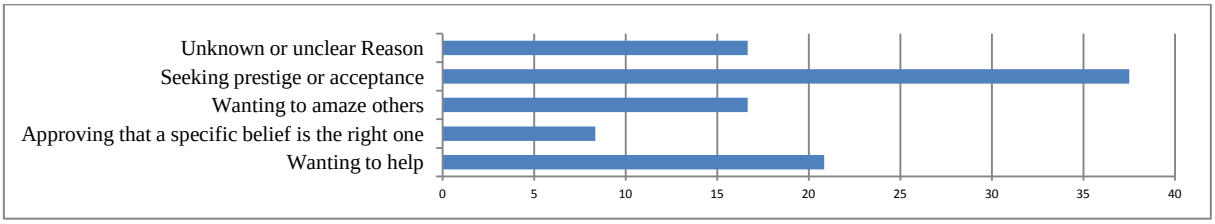

Figure 6. Percentages of Common Causes for Participation in Distributing SE Tricks

4.7 Common Reasons Why People Do Not Fall for Social Engineering Tricks

The current literature review suggests some commons countermeasures of social engineering such as training and education, policy and management, and auditing and testing. Our questionnaire results analysis also agreed that those countermeasures play vital roles in preventing people from falling for social engineering tricks and attacks. However, our questionnaire results show more countermeasures and factors that might help people in controlling their behaviors in SNSs. That is, some of the participants indicated some others reasons that made them aware of various deception tactics that occur in SNSs. For example, some participants stated that the way their family and parents have raised them made them aware of many tricks and helped them to control their behaviors when they deal with strangers. Moreover, some other participants stated that culture and social restrictions prevent them from going further in some behaviors such as seeking or making sexual-based relationships with others in SNSs. Finally, some participant shared that the fear of punishment by God, employer, spouse, or government helped them control their behaviors when they deal with strangers or when someone persuades them to make illegal action. Figure 7 shows what the questionnaire results which indicate the reasons why participants do not fall for social engineering tricks or behave in ways that would make them more susceptible to social engineering based attacks.

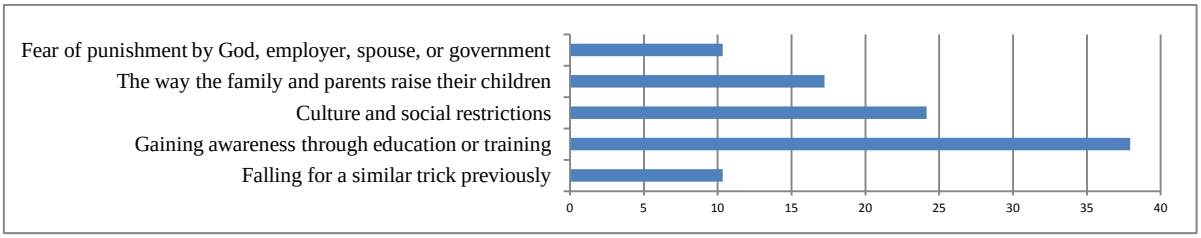

Figure 7. Percentages of Common Reasons Why People Do Not Fall for SS Tricks

5 DISCUSSION, LIMITATION, AND FUTURE WORK

It has been shown that SNSs can be dangerous weapons in hand of social engineers who use fake profiles, accounts, pages, and identities to entrap victims. This reflects the susceptibility of people and organizations falling victims to attackers who impersonate third parties and the susceptibility of people and organizations to identity theft by an attacker. Based in the result of this study, we suggest that impersonation is the key element of social engineering threats in SNSs. Because impersonation plays an important role in most of the social engineering threats such as phishing, identity theft, spamming, spaying, and reverse attacks, and because SNSs also lack effective techniques for predicting, detecting, or controlling such threats, researchers must find effective methods that help to eliminating them. As mentioned before, this study is part of a project that uses a *sequential exploratory mixed method* to predict a person's vulnerability to SE victimization based on his/her demographic variables such as age, gender, educational level, relationship status, and personality type. As shown in figure 8, for the qualitative phase, a *triangulation* approach, which involves the qualitative questionnaire-based survey (the present study), observations, and interviews will be used to explore the all possible factors that affect social engineering based attack in SNSs. For the second phase, the quantitative phase, we will use an experimental study to test our findings and to examine to what extent these factors can affect user victimization, and to link there factors to users' demographic variables.

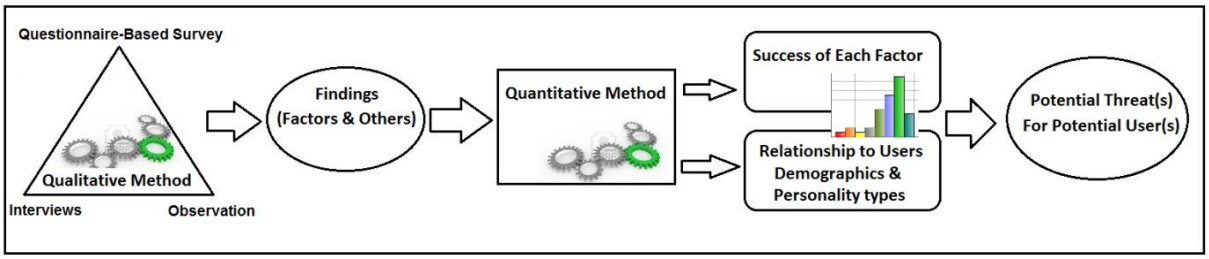

Figure 8. Full Project Design

The present study explored some parts of the phenomenon using questionnaire-based survey. While this work provides significant findings, there are two limitations worth noting. First, in order to encourage more participants to respond without feeling vulnerable or hesitant, we made our study with a very concise questionnaire-based survey with limited and focused questions. Therefore, it lacks the in-depth interactivity with the participants and richness of information that would give a fuller picture of potential hidden factors. However, this limitation should be eliminated by using the observations and interviews that will be conducted during the triangulation approach. The second limitation is that the present study did not investigate the existence of a relationship between the findings and users' demographics due to the small number of participants in this phase and because the aim of this study is exploratory only. However, this limitation should be eliminated by using the quantitative method in the second phase. Using a mixed methods design will ensure the validity and reliability of the study by illuminating the biases and subjectivity of the interpretation; such biases can occur in a qualitative study where the researcher has to interpret the data to explore the most important source characteristics.

References

Algarni , A., and Xu , Y. 2013. "Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models," *International Journal of e-Education, e-Business, e-Management and e-Learning* (3:6), p 7.

Algarni, A., Xu, Y., Chan, T., and Tian, Y.-C. Year. "Social engineering in social networking sites: Affect-based model," Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, IEEE2013a, pp. 508-515.

Algarni, A., Xu, Y., Chan, T., and Tian, Y.-C. 2013b. "Toward understanding social engineering," *Law & Practice: Critical Analysis and Legal Reasoning*, pp 279-300.

Bezuidenhout, M., Mouton, F., and Venter, H. Year. "Social engineering attack detection model: SEADM," Information Security for South Africa (ISSA), 2010, IEEE2010, pp. 1-8.

Braun, V., and Clarke, V. 2006. "Using thematic analysis in psychology," *Qualitative research in psychology* (3:2), pp 77-101.

Brody, R. G. 2012. "Flying under the radar: social engineering," *International Journal of Accounting and Information Management* (20:4), pp 335-347.

Chitrey, A., Singh, D., and Singh, V. 2012. "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model," *International Journal of Information and Network Security (IJINS)* (1:2), pp 45-53.

Cialdini, R. B. 2001. "Influence: Science and practice," *Boston: Allyn & Bacon*).

Corbin, J. M., and Strauss, A. 1990. "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative sociology* (13:1), pp 3-21.

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., and Rovira, E. 2012. "The Influences of Social Networks on Phishing Vulnerability,"), pp 2366-2373.

Creswell, J. W., Hanson, W. E., Plano, V. L. C., and Morales, A. 2007. "Qualitative research designs selection and implementation," *The Counseling Psychologist* (35:2), pp 236-264.

Darwish, A., Zarka, A. E., and Aloul, F. Year. "Towards understanding phishing victims' profile," Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on, IEEE2012, pp. 1-5.

Denzin, N. K., and Lincoln, Y. S. 2005. *The Sage handbook of qualitative research*, (Sage.

Dimensional-Research 2011. "The risk of social engineering on information security: a survey of it professionals," Technical Report, Long Beach, CA.

Gragg, D. 2003. "A multi-level defense against social engineering," *SANS Reading Room, March* (13).

Hogben, G. 2007. "Security issues and recommendations for online social networks," *ENISA position paper* (1).

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., and Pu, C. 2011. "Reverse social engineering attacks in online social networks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, pp. 55-74.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F. 2007. "Social phishing," *Communications of the ACM* (50:10), pp 94-100.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L. F., Hong, J., Blair, M. A., and Pham, T. 2009. "School of Phish: A Real-Word Evaluation of Anti-Phishing Training (CMU-CyLab-09-002),").

Kvedar, D., Nettis, M., and Fulton, S. P. 2010. "The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition," *Journal of Computing Sciences in Colleges* (26:2), pp 80-87.

Marett, K., Biros, D. P., and Knode, M. L. 2004. "Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training," in *Intelligence and Security Informatics*, Springer, pp. 187-200.

Mitnick, K. D., and Simon, W. L. 2001. *The art of deception: Controlling the human element of security*, (Wiley.

Mohebzada, J., El Zarka, A., and Bhojani, A. 2010. "COE444 Spring 2010: Research Project Report,").

Nagy, J., and Pecho, P. 2009. "Social Networks Security,"), pp 321-325.

Nohlberg, M. 2008. "Securing information assets: understanding, measuring and protecting against social engineering attacks,").

Parrish Jr, J. L., Bailey, J. L., and Courtney, J. F. 2009. "A Personality Based Model for Determining Susceptibility to Phishing Attacks," *Little Rock: University of Arkansas*).

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., and Butavicius, M. 2012. "Why do some people manage phishing e-mails better than others?," *Information Management & Computer Security* (20:1), pp 18-28.

Peltier, T. R. 2006. "Social engineering: concepts and solutions," *EDPACS* (33:8), pp 1-13.

Richardson, R. L. 2007. *CSI survey 2007: The 12th annual computer crime and security survey*, (Computer Security Institute.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. Year. "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," Proceedings of the 28th international conference on Human factors in computing systems, ACM2010, pp. 373-382.

Strauss, A., and Corbin, J. 1998. "Basics of qualitative research: Procedures and techniques for developing grounded theory," Thousand Oaks, CA: Sage.

Twitchell, D. P. Year. "Social engineering in information assurance curricula," Proceedings of the 3rd annual conference on Information security curriculum development, ACM2006, pp. 191-193.

Workman, M. 2008. "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security," *Journal of the American Society for Information Science and Technology* (59:4), pp 662-674.

Zhang, C., Sun, J., Zhu, X., and Fang, Y. 2010. "Privacy and security for online social networks: challenges and opportunities," in *Network, IEEE*, pp. 13-18.