2014 IEEE International Conference on Services Computing

Social Engineering in Social Networking Sites:
The Art of Impersonation

Abdullah Algarni, Yue Xu, Taizan Chan
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
abdullahayedm.algarni@student.qut.edu.au, yue.xu@qut.edu.au, t.chan@qut.edu.au

***Abstract*—Social networking sites (SNSs), with their large number of users and large information base, seem to be the perfect breeding ground for exploiting the vulnerabilities of people, who are considered the weakest link in security. Deceiving, persuading, or influencing people to provide information or to perform an action that will benefit the attacker is known as "social engineering." Fraudulent and deceptive people use social engineering traps and tactics through SNSs to trick users into obeying them, accepting threats, and falling victim to various crimes such as phishing, sexual abuse, financial abuse, identity theft, and physical crime. Although organizations, researchers, and practitioners recognize the serious risks of social engineering, there is a severe lack of understanding and control of such threats. This may be partly due to the complexity of human behaviors in approaching, accepting, and failing to recognize social engineering tricks. This research aims to investigate the impact of source characteristics on users' susceptibility to social engineering victimization in SNSs, particularly Facebook. Using grounded theory method, we develop a model that explains what and how source characteristics influence Facebook users to judge the attacker as credible.**

Keywords*—social engineering; social networking sites; information security management; source credibility; trust management; impersonation

I. Introduction

Since the first recognizable appearance of social networking sites (SNSs) in 1997, with the SNS SixDegrees.com [1], people have been attracted to these sites to construct their profiles and to communicate with each other in different ways depending on the nature of the site. SNSs have also implemented a wide variety of technical features that enable people, companies, organizations, and governmental institutions to do a variety of services [1]. As the number of SNS users has been increasing dramatically, so has the amount of sensitive and private information on people, companies, organizations, and governmental institutions. This not only makes SNSs attractive to faithful users but also makes SNSs the perfect breeding ground for malicious users and attackers. Information is always under threat; it can be intercepted, modified, or exposed. The facilities that have been set up to monitor such attacks are also constantly under attack [2]. Such attacks shape the challenges of providing usability and sociability, which are the main purposes of SNSs, and of ensuring integrity, confidentiality, and availability, which are standard principles of security.

Social engineering (SE) is the art of deceiving or tricking people to help attackers reach their goals, to gain information from them, or to persuade them to perform an action that will benefit the attacker in some way [3]. Because of the incredible complexity of social engineering, it has become an important problem in information security. The Institute of Management and Administration (IOMA) reported that social engineering was the top security threat in 2005. Social engineering threats are on the rise despite continued improvements in protection against technology-based threats [4]. According to a survey by Dimension Research (2011) on 850 IT and security professionals in the United States, Canada, the United Kingdom, Germany, Australia, and New Zealand, 48% of the participants had been victims of social engineering attacks. Of the participants, 39% believed the SNSs were the most common source of social engineering threats [5].

Research shows that people are more likely to obey and accept a message when the source presents itself as credible [6]. *Source credibility* is a multidimensional concept that enables the receiver to rate the source in relation to the information. This rating correlates with the capability of the receiver to attribute reality, truth, and substance to the information, and to make a global evaluation of the believability of the information source [7]. This study aims to investigate the impact of source characteristics on social engineering (SE) victimization on SNSs, particularly Facebook. The study aims to discover how Facebook users determine whether they are encountering an attacker or a legitimate user based on his/her characteristics. A model is developed to explain what and how source characteristics influence Facebook users to judge the attacker as a credible.

II. Source Characteristics and Susceptibility to SE Victimization

Social engineering always comes as a message containing a request. This request can be direct, or it can be a trick that requires the victim to accept or respond to the request [8]. For decades, marketers, advertisers, politicians, professionals of various areas, and researchers in many fields have investigated the effects of source characteristics on changing the beliefs, attitudes, or behaviors of the audience toward accepting a message. A highly credible source is commonly found to

978-1-4799-5066-9/14 $31.00 © 2014 IEEE
DOI 10.1109/SCC.2014.108

induce more persuasion toward the acceptance of the message than a low-credibility one [9]. According to source credibility theory, people are more likely to obey and accept a message when the source presents itself as credible [6].

Moreover, in several phishing studies, the effectiveness of (false) source credibility has been repeatedly demonstrated in phishing victimization [10-12]. Those studies found that phishing offenders often employ source credibility. The same tricks are observed in cases of social engineering in SNSs, where the ability of the social engineer to launch the attack involves wearing a suitable "hat" and playing a suitable character [13]. This character can be a very poor person, a sexy girl, an authority, a celebrity, a wonderful friend, and so on. A social engineer can also impersonate a real person whom the victim knows well, such as a friend, boss, relative, or even a famous person. This task is much easier in SNSs where attackers can create multiple fake profiles and choose their names, photos, locations, and other details easily. At the same time, it is more difficult for the victim to uncover the deception through an SNS than in a face-to-face, real-life situation.

III. Theoretical Background of Source Credibility

Credibility is a communication phenomenon where communication occurs between at least two parties [14]. Credibility research has its roots in persuasion, especially in human communication research. Source credibility theory views credibility as the degree to which a source meets a receiver's needs [6]. Persuasion is comprised of the following three main elements: the sender or the source, the mean or the message, and the recipient [15]. In the case of social engineering in SNSs, the sender is the social engineer or the attacker, the message is the trick or the technique, and the recipient is the user. Realizing that source credibility is a multidimensional concept, several studies have investigated its dimensions using explorative factor analysis. Most of those studies provided their participants with a number of semantic differential items with which to rate the credibility of the sources. The resulting data were then combined into factors through factor analysis. The factors were interpreted as dimensions of credibility.

Source credibility has been well investigated in marketing research that focuses on which factors people base their judgments of the credibility of the salesperson or spokesperson. Social engineers and online marketers persuade people for different reasons. The marketers want to convince potential buyers to make purchases, while social engineers aim at obtaining valuable information or other kinds of benefits [16]. An experiment conducted by Workman (2007) used the analysis of a threat and the elaboration probability to examine its usability to provide an explanation of deception [17]. The results of this experiment can help explain how the same factors can be used in social engineering. Eisend (2006) summarized 28 major source credibility studies and examined whether a generalized conceptualization of credibility of various sources in marketing communication exists [14]. These studies suggest three main common dimensions:

1) Sincerity or trustworthiness, including character and personal integrity
2) Professionalism or competence, including expertise, knowledge, ability, and qualifications
3) Attraction or appearance of the source, including dynamism, attractiveness, and presentation

Considering these potentially important variables suggested in marketing communication research, the questions that need to be addressed are:

1) What are the main dimensions of source credibility in terms of social engineering in Facebook?
2) What source characteristics influence Facebook users to judge the attacker as credible?

IV. Methodology

This study investigates the impact of source characteristics on users' susceptibility to social engineering victimization in SNSs by exploring how Facebook users distinguish between attackers and legitimate users based on their characteristics. As explained in the previous section, the variables that exist in the literature were developed and tested mostly in marketing research. In this situation, when no existing theory or model can be applied to address the research questions, Creswell (2012) suggests using the grounded theory method to inductively build the targeted theory or model [18].

The challenge of the research topic is that the participants would probably claim that they are aware of deception and cannot be deceived. At best, they would admit that they do not know how they get deceived. Research indicates that people perform poorly in detecting social engineering attacks [19, 20]. Research also suggests that social engineers could succeed even among organizations that claim to be aware of social engineering techniques [21]. It is also possible for participants who have experienced social-engineering-based attacks in SNSs to feel hesitant to report their stories.

For this kind of challenge, Flick (2004) suggests using multiple sources of data [22]. The multiple sources used in this research include in-depth interviews and observations of participants' profiles and timelines. The purpose, limitations, and procedures of these two methods will be explained in detail in the following sections.

A. Observations of Participants' Profiles and Timelines

Although an interview is a highly efficient way to gather rich empirical data, it can present challenging biases. Interviews are conducted in a social context that is not anonymous. Therefore, participants may present themselves in a certain light to the interviewer rather than report their actual experience. For this reason, Strauss and Corbin (1990, 1998) suggest collecting and analyzing observations or documents as a supporting method to interviews [23, 24]. According to Eisenhardt (2007), a "key approach to mitigating bias is to combine retrospective and real-time cases … real-time cases employ longitudinal data collection of interviews and, often, observations, both of which help to mitigate retrospective sensemaking and impression management" [25].

Facebook profiles and timelines save and keep a record of individuals' activities in their accounts and their interactions with other Facebook users, such as sharing, posting, liking, and commenting. They also show the user's friends, groups, events, and commercial pages. Before interviews were conducted, the researcher made "online observations" of the participants' behaviors by observing their accounts (profiles and timelines) with their permission. This allowed the researcher to obtain an actual picture of their previous and actual behaviors, to gain a better idea of what to ask in the interview, and to make better sense of the participants' responses. Moreover, some of the participants might have fallen prey to social engineering tricks without understanding how they fell for the tricks or without even being aware that they were tricked. The notes taken during the observations also helped in the discussion of the participants' various issues during the in-depth interviews.

B. *Interview Approach*

The interview is a research method used to gain a deep understanding of human behavior and the different reasons governing the behavior. Interviews are conducted to understand a research topic or problem from the perspective of the population that is involved. Since the literature lacks a theory or model that can be used to address the research questions, grounded theory will be used as suggested by Creswell (2012) to inductively build the targeted model. According to Creswell (2012), the two popular approaches to grounded theory are the systematic procedures of Strauss and Corbin (1990, 1998) [23, 24] and the constructivist approach of Charmaz (2006) [26].

In this study, the systematic procedures of Strauss and Corbin (1990, 1998) is chosen to be used because they are compatible with the purpose of this study, which is to systematically develop a model that contains and explains the source characteristics. Using this approach, the researcher conducts 20 to 30 interviews to collect data that saturate the categories or themes [23]. The category is the unit of information; in this case, the categories are the main dimensions of the factors that influence the users' judgment of source credibility. The researcher in this approach keeps trying to find information to add to the themes until no more can be found [18]. This approach also involves collecting and analyzing observations and documents.

C. *Interview Analysis and Coding*

The aim of analysis and coding is to categorize the data into themes, categories, or factors. Strauss and Corbin (1990, 1998) suggest that the researcher begin the analysis while collecting data. 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) [23, 24]. Finally, the researcher performs "selective coding," which seeks to develop hypotheses that are interrelated with the categories in the model. In the first phase of analysis, the researcher used a manual method of color coding and note taking. NVIVO software, which is a qualitative research analysis tool, was used as in the second phase to analyze the transcripts for more accurate results.

D. *Pilot Interviews*

A pilot study is a rehearsal study that is conducted before the main study [27]. Four pilot interviews were conducted to test the proposed interview protocol for its clarity and effectiveness in exploring participants' experiences of the phenomenon being studied. The interview protocol was adapted based on the definition and examples of social engineering in SNSs. Some modifications were made to the interview questions in light of the pilot interview results. The major change that resulted from the pilot interviews was the addition of the observation method to the research design. After the first two pilot interviews, it was clear that observing the participants' profiles and timelines would give the researcher a more comprehensive picture of their actual behaviors, a better idea of what to ask in the interviews, and a better understanding of the interview responses. Therefore, observations were incorporated into the study before conducting the last two pilot interviews. The adjustments that were made based on the results of the pilot interviews have enabled the project to proceed in conformity with the research aim and in accordance with the methodology.

E. *Interview Sampling*

The systematic procedures of Strauss and Corbin (1990, 1998) use "theoretical sampling," in which the researcher chooses the participants selectively and theoretically. This helps the researcher best form the theory [23, 24]. A. Algarni et al., (2013) suggest that people who deal with social engineering in SNSs are affected by *risk beliefs factors*, *Socio-psychological factors, and Countermeasures factors* [28]. Those factors, (as shown in Fig. 1), are affected by other sub-factors such as previous experience, awareness level, personality type, and user demographics.

Participants with different personality types and demographic variables were selected to ensure that the sample represents a potentially high degree of variation and to increase the likelihood of identifying all possible factors under investigation. A letter of invitation was sent to various organizations asking the directors if they would be willing to disseminate it to their personnel. As shown in Table 1, 20 interviews and four pilot interviews were conducted. The employees in the sample were purposively chosen from two different international organizations, from different cultural heritage (Saudi, American, Indian, Egyptian, and Jordanian), and their participation was voluntary. One of these organizations experienced a serious cyber attack two years ago and has since started to train its employees on the various types of cyber threats including social engineering threats. In contrast, the second organization has not yet experienced a serious cyber attack, so it has not trained its employees about social engineering. Thus, the participants have different risk beliefs and different levels of awareness regarding social engineering.

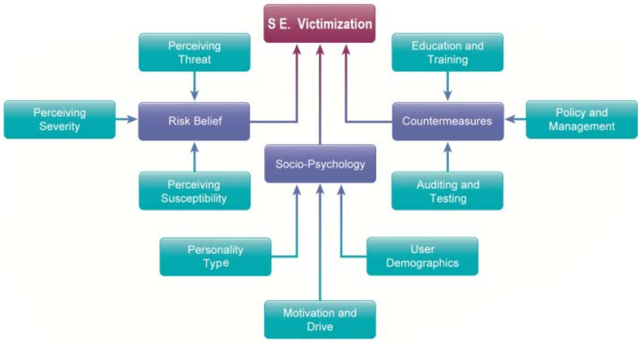

Figure 1. Factors in the Selection of the Theoretical Sample.

TABLE 1. CHARACTERISTICS OF THE INTERVIEW SAMPLE

Age				Gender		Personality Type					Employment			Educational Level			
<21	21-30	31-40	>40	Male	Female	Extraverted	Agreeable	Conscientious	Neurotic	Open	Organization 1	Organization 2	Pilot	Undergraduate or Lower	Bachelor's Degree	Master's Degree	Doctoral Degree
3	7	10	4	13	11	4	6	4	3	7	10	10	4	3	11	6	4

F. *Interview Protocol*

Semi-structured questions were prepared to address the main topics under investigation. For some participants, more questions were added based on the observations of their profiles and timelines. In addition, as mentioned by Wengraf (2001), the interactivity with the participants allows the interviewer to tackle important questions and topics that were not covered by the semi-structured questions [29]. The interviews were conducted face to face, audio recorded, and then transcribed. Each interview took 30 to 60 minutes. The researcher's roles included conducting, recording, and transcribing the interviews, which were conducted in Arabic. The task of transcribing the interviews that were conducted in English was assigned to a commercial office. All the activities of this study were categorized under "Low Risk Applications" in accordance with the National Statement on Ethical Conduct in Research Involving Humans. The research application for low risk research involving human participants was approved by the Human Research Ethics Committee of Queensland University of Technology.

V. FINDINGS

The data collected from observations and interviews showed significant source characteristics that influence Facebook users to judge the attacker as credible, thus making them susceptible to social engineering victimization. These source characteristics can be categorized under four main dimensions: perceived sincerity, perceived competence, perceived attraction, and perceived worthiness. The first three dimensions have been observed and reported in communication and marketing research. However, the fourth dimension (perceived worthiness) is a new dimension that emerged in this study. The following sections will explain the impact of source characteristics on social engineering victimization in Facebook, the four dimensions of these characteristics, and how users judge credibility based on variables that exist in the Facebook environment.

A. *The Impact of Source Characteristics on SE Victimization*

The data show that source credibility affects users' susceptibility to social engineering victimization in two main stages: approaching the social engineering message and judging or deciding whether to accept the message (Fig. 2). In the approaching stage, when users log in to their Facebook accounts, they encounter many messages such as posts, news, links, photos, videos, applications, or stories that are written, suggested, liked, or shared by others. The sources of these messages are not necessarily well known to the user in real life; they can be friends that the user knows only in Facebook, friends of friends, members of a group or event in which the user is a member, or strangers who post in a fan or commercial page of which the user is a member. Therefore, the user does not pay the same attention to all the content or messages encountered. The interview data show that source credibility is one criterion by which the user approaches the content or message. For instance, Participant 5 shared, "Yes, there are some friends whose posts I like to read, even if I don't have enough time and regardless of the topic that they are talking about." The second impact of source characteristics is on the user's judgment or decision on whether to accept the message. Source credibility was also reported as one criterion that is used to decide whether to accept the message:

> Interviewer (I): If someone asks you a favor, such as a donation, document, software, or participation, would you accept?
> Participant (P): Well, that depends on the person who asked me the favor and the request itself.
> I: Can you explain the criteria that you use to decide whether to help or not?
> P: What I mean is that, with some people, I would think carefully before I reject their requests … also, there are some requests that I cannot grant or that could cost me a lot … in a situation like that, I think I would probably choose what would do me the least harm—granting the request or losing the person. (Participant 8)

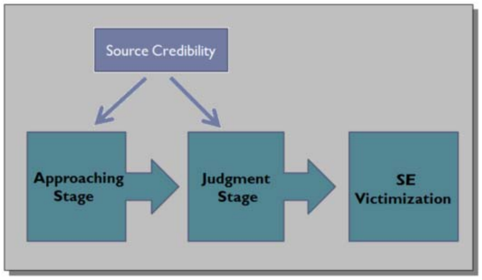

Figure 2. How Source Credibility Affects SE Victimization

B. Characteristics Related to the Dimension of Sincerity

Source characteristics related to sincerity were repeatedly mentioned in the interviews. The characteristics under this dimension include honesty, trustworthiness, and believability. For instance, Participant 2 explained that honesty is her primary criteria in deciding whether to accept or reject a request:

> I: If someone asks you a favor, such as a donation, document, software, or participation, would you accept? What criteria would you use to decide to accept or reject the request?
> P: The first thing I would think about is honesty … you know, I have to make sure that he is not lying to me.

Participants also cited some factors that they consider when judging a Facebook user's sincerity. For example, when Participant 3 suspects that the user is a scammer, he usually looks at the user's number of friends and the amount of content in the user's account:

> I: What kind of friend request do you usually accept? What criteria would you use to decide whom to accept or reject?
> P: If it is not clear who the person is, the request can wait, maybe until I remember who the person is. If I'm certain that it is a scammer, I would make sure that it is not a fake profile by checking the user's number of friends and the amount of content in the user's account.

Participant 1 also mentioned that when she receives a friend request from a stranger, she checks if they have any common friends:

> I: What kind of friend request do you usually accept? What criteria would you use to decide whom to accept or reject?
> P: When I see that we have common friends, I say to myself, "Maybe the system suggested that he add me to his friend list," so I accept the invitation.

Participants 5 and 2 reported another factor that reflects sincerity, namely common beliefs:

> You are just sort of blind in Facebook. You don't know if what someone is saying in his profile is true … I would discover his attitude by observing his profile and checking if he really believes in what I believe. (Participant 5)

> As you know, there are many political and religious persecutions and issues now, so having the same religion can make you sympathize with someone. I think it encourages you to help. (Participant 2)

Finally, the use of a nickname has been cited as a suspicious sign. Therefore, the use of a person's real name or a common name can reflect sincerity. For instance, Participant 16 indicated that he does not trust people who use nicknames:

> I would suspect that, in the vast majority of cases, users who use nicknames are trying to be cute. I think they are trying to hide their reality from others, and there must be a reason for that. If a person is quite confident about his attitude, he would not hide his real identity.

C. Characteristics Related to the Dimension of Competence

The second dimension of source characteristics influencing Facebook users to judge others as credible is the user's competence or power. This concept represents the quality of being adequacy and possession of required skill or capacity. Three characteristics observed in the data reflect the dimension of competence: qualifications, celebrity, and wealth.

Participant 11 indicated that he looks at SNSs including Facebook as a good, free environment to form a network of qualified people from all over the world:

> I don't know if you agree with me or not, but I think that the primary benefit of social networks including Facebook is that they allow you to build a network of qualified and expert people in your field. The only thing you need to do is send them a friend request. You lose nothing if they reject it!

Another example regarding celebrity was observed in the account of Participant 15. Through observation, the researcher found that she liked (i.e., followed or subscribed to) more than 40 celebrities from different countries and in different areas such as sports, writing, acting, music, and fashion. She explained this as follows:

> P: I love to follow every aspect of celebrities' lives, but I don't think I'm the only one who does this. I have some friends who have entire conversations on the subject of celebrities, such as their marriages, divorces, and travels.
> I: If you come across a request from one of these celebrities, such as an invitation to participate to win a prize, or a request for a donation to a charitable organization, do you think that their being a celebrity will have a different effect on your decision?
> P: I think so. You know, we always see them on TV, in the newspapers, and in the movies. They have become a part of our lives. I consider it reasonable to find myself trusting them or eager to communicate with them.

The third characteristic related to competence is wealth. Participant 13 shared a friend's bad experience in which a scammer deceived her by pretending to be wealthy:

> One of my friends used to know a man on Facebook who pretended to be a rich person. After a couple of months of chatting with each other on Facebook, he said that his business was in trouble and that he needed to borrow a couple of thousand dollars from her. Unfortunately, my friend trusted him and gave him the money. Immediately after receiving the money, the man removed her from his friend list and disappeared.

D. Characteristics Related to the Dimension of Attraction

The dimension of attraction represents the feature or the quality that evokes interest and liking. Two characteristics observed in the data reflect the dimension of attraction: good looks and good writing skills. For instance, Participant 6 mentioned the positive effect of a user's good looks:

“Interaction with good-looking girls makes me feel good. I get an overall feeling of confidence.”

Participant 1 also mentioned the impact of looks on her judgment. She said that the first thing she looks at when she wants to know more about somebody on Facebook is the user’s photos:

> I: Do you think that being good- or bad-looking has any impact on your judgment?
> P: In a real life situation, it’s about attitude and personality and probably not about how bad-looking one is. But on Facebook, I would look at the photos initially to get a first impression.

Good writing skills were also identified as a vital factor that attracts others and reflects the credibility of the source:

> I spend most of my time on Facebook reading others’ posts or comments, so the first thing that attracts me is good writing. When I see an impressive post or comment, I immediately look at the profile of the person who wrote it, and sometimes I send the person a friend request. (Participant 18)

E. Characteristics Related to the Dimension of Worthiness

Some participants mentioned the worthiness of the source as an important dimension to consider when deciding whether to accept or reject a request. They believe that the source must be worthy of their acceptance or response, even if they believe the source is sincere. The worthiness is having or showing the qualities that deserve effort, attention, respect or the specified action or regard. For instance, Participant 1 said, “If I care about him so much, I’m willing to do anything for him; I support him financially, and do everything I can for him.”

In addition, some participants mentioned factors of the users’ worthiness, namely authority, sexual compatibility, and reciprocity. The authority is the power over the recipient and the right to make decisions. Participant 2, for example, feels compelled to react to her boss’ posts: “When I see a post from my boss, I feel hesitant to leave it without commenting, sharing, or at least clicking the ‘like’ button.”

The sexual compatibility is the degree to which a couple perceives they share sexual preferences or desires. The observations revealed that participant 14 wrote a “sexual” reference in his profile. When asked why he wrote it, he explained that he wanted to weed out poor matches:

> I wrote it explicitly because I had some experiences where I got together with a girl and we both liked each other, but it turned out that I really liked sex and she did not. So I wrote that in the profile to kind of weed out those people … If I have a chance to have a sexual relationship with someone I want, and I know that accepting the request will make it happen, I would accept it. I think anybody who says differently is lying.

Reciprocity is the cooperative interchange of favors or privileges. It has been observed that it also plays an important role in judging credibility in Facebook. Complimenting, commenting on, or liking another user’s posts can build a credible relationship between users, thus encouraging them to accept each other’s requests. As Participant 9 shared,

> P: Some of the users in my friend list always like and write good comments on my photos or posts, and I usually do the same for them to keep them around.
> I: How about if they ask you for something, such as money or sensitive information?
> P: As I mentioned before, it depends on the amount of money or the type of information, but generally speaking, I would try to make them happy and maintain a positive appearance for them.

VI. Discussion

This study identified 13 source characteristics that influence Facebook users to judge an attacker as credible. These characteristics render Facebook users susceptible to attackers, who can use fake profiles, accounts, pages, and identities to entrap victims. Individuals’ social and psychological factors significantly influence their susceptibility to various types of fraud and attacks. By exploiting human needs and drives, attackers can launch many forms of attacks through deceit, manipulation, and dishonesty. It has been observed that Facebook users judge source credibility based on their desire for money, prestige, compliments, sex, belonging, and friendship, as well as their desire to help. Thus, people and organizations are susceptible to fall victim to identity theft and to attackers who take on identities that can satisfy the victim’s desires.

Considering the research aim which is exploring what source characteristics influence Facebook users to judge the attacker as credible, thirteen source characteristics, as shown in Fig.3, were found to be critical: 1) number of friends, 2) common friends, 3) amount of content in the source’s account, 4) common beliefs, 5) the use of source’s real name, 6) qualifications, 7) celebrity, 8) wealth, 9) good looks, 10) good writing skills, 11) authority, 12) sexual compatibility, and 13) reciprocity. Based on these thirteen source characteristics, a priori model was developed as shown in Fig. 4.

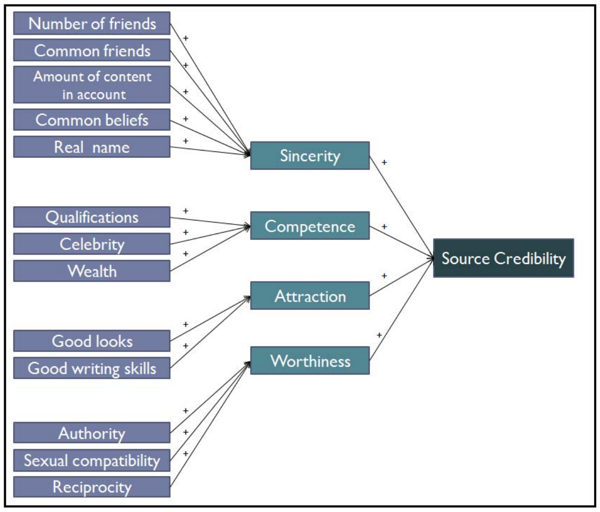

Figure 3. How People Judge Source Credibility in Terms of Social Engineering in Facebook

The hypotheses regarding the impact of source characteristics on users' susceptibility to social engineering victimization are:

H1: Users are more susceptible to SE victimization by attackers who pretend to have more friends.
H2: Users are more susceptible to SE victimization by attackers who pretend to have more friends in common with them.
H3: Users are more susceptible to SE victimization by attackers who pretend to have more profile content.
H4: Users are more susceptible to SE victimization by attackers who pretend to have the same beliefs or religion.
H5: Users are more susceptible to SE victimization by attackers who pretend to use their real names.
H6: Users are more susceptible to SE victimization by attackers who pretend to be qualified.
H7: Users are more susceptible to SE victimization by attackers who pretend to be celebrities.
H8: Users are more susceptible to SE victimization by attackers who pretend to be wealthy.
H9: Users are more susceptible to SE victimization by attackers who pretend to be good looking.
H10: Users are more susceptible to SE victimization by attackers who pretend to be a good writer.
H11: Users are more susceptible to SE victimization by attackers who pretend to have authority over them.
H12: Users are more susceptible to SE victimization by attackers who pretend to be sexually compatible with them.
H13: Users are more susceptible to SE victimization by attackers who pretend to like their posts and activities or compliment them through comments and posts.

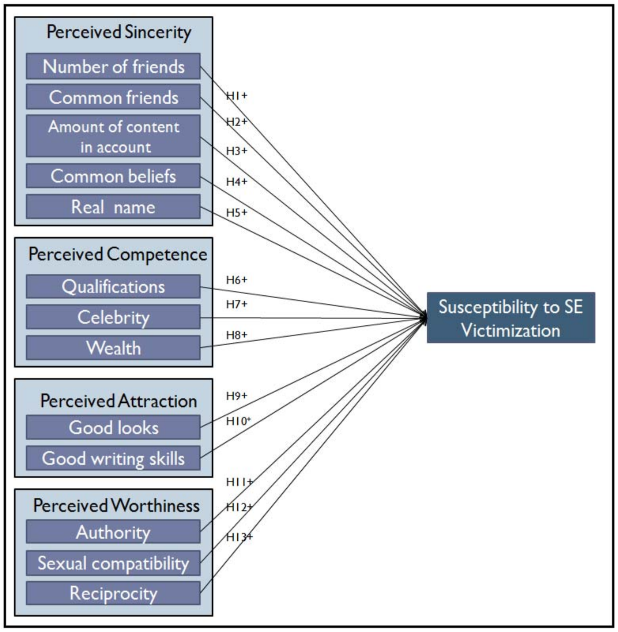

Figure 4. A Priori Model of the Impact of Source Characteristics on Users' Susceptibility to SE Victimization in Facebook

The findings show some key technical factors of Facebook that can help attackers easily impersonate a credible source, abuse users' behaviors, and mislead their judgment. These factors include the lack of authentication, exposure to strangers, the lack of filtering, the lack of privacy, platform for all kinds of sources such as celebrities, rich people, royalty, politicians, and companies; and the fast spread of tricks through sharing, liking, commenting, or posting in a group or page. Several companies have adopted SNSs to promote collaboration among employees, to communicate with customers, and to advertise products and services. Although social engineering is one of the most significant security risks in information security, it has largely been ignored in information systems, especially concerning SNSs. Because impersonation plays an important role in most of the social engineering threats such as phishing, identity theft, spamming, spying, and reverse attacks, and because SNSs lack effective techniques for predicting, detecting, or controlling such threats, researchers must find effective methods to help eliminate them.

VII. Limitations and Future Research

This study is part of a project that attempts to predict a person's vulnerability to social engineering victimization based on his/her demographic variables such as age, gender, educational level, relationship status, and personality type. The present study explored source characteristics that influence Facebook users to judge an attacker as credible. However, qualitative methods cannot determine the existence of a relationship between these factors and users' demographics due to the small number of participants in this phase.

To predict the potential threats to the users based on their demographics, and to test the study hypotheses and the a priori model (Fig. 4), a quantitative method will be used in the second phase. This type of mixed methods design that starts with a qualitative method followed by a quantitative method is known as the sequential exploratory mixed method [30]. 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.

VIII. Conclusion

After Social engineering has become an important problem in information security, especially in new environments such as SNSs, owing to factors of SNSs that reduce the users' ability to detect the attack and increase the attackers' ability to launch it. Due to the vital role of source credibility in changing beliefs, attitudes, and behaviors, this study investigated the impact of source characteristics on users' susceptibility to social engineering victimization in Facebook. Based on the findings of this study, a model was developed to explain what and how source characteristics influence Facebook users to judge the attacker as credible. Thirteen source characteristics were found to be critical in judging source credibility: 1) number of friends, 2) common friends, 3) amount of content in the source's account, 4) common beliefs, 5) the use of source's real name, 6) qualifications, 7) celebrity, 8) wealth, 9) good looks, 10) good writing skills, 11) authority, 12) sexual compatibility, and 13) reciprocity. The findings of this research contribute to the knowledge of social engineering, SNS security, and individual or organizational information security management. The findings also provide a substantial foundation for several directions of research aimed at uncovering deception and scams in SNSs, such as data mining, social networking development, privacy protection, and trust management.

References

[1] N. B. Ellison, "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication,* vol. 13, pp. 210-230, 2007.

[2] C. Zhang, J. Sun, X. Zhu, and Y. Fang. (2010, 4). *Privacy and security for online social networks: challenges and opportunities*.

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

[4] S. T. Thompson, "Helping the hacker? Library information, security, and social engineering," *Information Technology and Libraries,* vol. 25, pp. 222-225, 2013.

[5] Dimensional-Research, "The Risk of Social Engineering on Information Security: a Survey of IT Professionals," Technical Report, Long Beach, CA2011.

[6] C. I. Hovland, I. L. Janis, and H. H. Kelley, "Communication and persuasion; psychological studies of opinion change," 1953.

[7] C. I. Hovland and W. Weiss, "The influence of source credibility on communication effectiveness," *Public opinion quarterly,* vol. 15, pp. 635-650, 1951.

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

[9] C. Pornpitakpan, "The persuasiveness of source credibility: A critical review of five decades' evidence," *Journal of Applied Social Psychology,* vol. 34, pp. 243-281, 2004.

[10] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581-590.

[11] X. R. Luo, W. Zhang, S. Burd, and A. Seazzu, "Investigating Phishing Victimization with the Heuristic-Systematic Model: A Theoretical Framework and an Exploration," *Computers & Security,* 2012.

[12] S. W. Sussman and W. S. Siegal, "Informational influence in organizations: an integrated approach to knowledge adoption," *Information Systems Research,* vol. 14, pp. 47-65, 2003.

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

[14] M. Eisend, "Source credibility dimensions in marketing communication-a generalized solution," *Journal of Empirical Generalizations in Marketing,* vol. 10, pp. 1-33, 2006.

[15] D. J. O'Keefe, *Persuasion: Theory and research* vol. 2: SAGE Publications, Incorporated, 2002.

[16] G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in *Proceedings of the 5th conference on Information technology education*, 2004, pp. 177-181.

[17] M. Workman, "Gaining access with social engineering: An empirical study of the threat," *Information Systems Security,* vol. 16, pp. 315-331, 2007.

[18] J. W. Creswell, *Qualitative inquiry and research design: Choosing among five approaches*: Sage, 2012.

[19] T. Qi, "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering," in *Intelligence and Security Informatics, 2007 IEEE*, 2007, pp. 152-159.

[20] S. Grazioli, "Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet," *Group Decision and Negotiation,* vol. 13, pp. 149-172, 2004.

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

[22] U. Flick, "Triangulation in qualitative research," *A companion to qualitative research,* pp. 178-183, 2004.

[23] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative sociology,* vol. 13, pp. 3-21, 1990.

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

[25] K. M. Eisenhardt and M. E. Graebner, "Theory building from cases: opportunities and challenges," *Academy of management journal,* vol. 50, pp. 25-32, 2007.

[26] K. Charmaz, *Constructing grounded theory: A practical guide through qualitative analysis*: Pine Forge Press, 2006.

[27] M. D. Myers, "Qualitative research in information systems," *Management Information Systems Quarterly,* vol. 21, pp. 241-242, 1997.

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

[29] T. Wengraf, *Qualitative research interviewing: Biographic narrative and semi-structured methods*: Sage, 2001.

[30] A. Tashakkori and C. Teddlie, *Handbook of mixed methods in social & behavioral research*: Sage, 2003.