Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook

Completed Research Paper

Abdullah Algarni
Science and Engineering Faculty
Queensland University of Technology
Brisbane, Australia
abdullahayedm.algarni@student.qut.edu.au
Institute of Public Administration
Saudi Arabia
algarniaa@ipa.edu.sa

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

Taizan Chan
Science and Engineering Faculty
Information Systems
Queensland University of Technology
Brisbane, Australia
t.chan@qut.edu.au

Abstract

Past research has suggested that social engineering poses the most significant security risk. Recent studies have suggested that social networking sites (SNSs) are the most common source of social engineering attacks. The risk of social engineering attacks in SNSs is associated with the difficulty of making accurate judgments regarding source credibility in the virtual environment of SNSs. In this paper, we quantitatively investigate source credibility dimensions in terms of social engineering on Facebook, as well as the source characteristics that influence Facebook users to judge an attacker as credible, therefore making them susceptible to victimization. Moreover, in order to predict users' susceptibility to social engineering victimization based on their demographics, we investigate the effectiveness of source characteristics on different demographic groups by measuring the consent intentions and behavior responses of users to social engineering requests using a role-play experiment.

Keywords: Social engineering, deception, source credibility, phishing, Facebook

Introduction

Security threats in information systems generally come through the vulnerabilities of technologies or the vulnerabilities of people. People are considered the weakest link in security (Nohlberg 2009; West et al. 2009). *Social engineering* is the art of deceiving or tricking people in order to gain information from them, or to persuade them to perform an action that will benefit the attacker in some way (Hadnagy 2010; Thornburgh 2004; Workman 2007). Many organizations recognize the importance of predicting and controlling social engineering, but many fail to reach that goal (Brody 2012). Recently, fraudulent and deceptive people have been using social engineering traps and tactics by 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. The simple trick of offering free cell phone minutes, accounted for the largest number of attacks on Facebook users in 2013, increasing from 56% in 2012 to 81% in 2013 (Toops 2014). Recent research on SNSs security showed that most social engineering threats, such as spamming, identity cloning, and social bots, rely mainly on fake identities (Fire et al. 2014). This provides an explanation for why around 83 million (8.7% of all accounts) Facebook accounts are estimated to be fake (Couper 2013). Several researchers have investigated and highlighted the risks associated with social engineering in SNSs (e.g., (Nagy and Pecho 2009; Jagatic et al. 2007; Dimensional-Research 2011; Chitrey et al. 2012; Algarni et al. 2013a; Algarni et al. 2013b; Braun and Esswein 2013)). These studies have suggested that SNSs are the most common source of social engineering threats nowadays.

The risk of social engineering attacks in SNSs is associated with how difficult it is for users to make accurate judgments regarding deception in the virtual environment of SNSs. In our previous work, (Algarni et al. 2014a), and (Algarni et al. 2014b), we investigated how people perceive and make judgments about the credibility of attackers in Facebook, which is the key element in a user's decision to accept or reject social engineering attacks. Using a qualitative grounded theory method, we explored source credibility dimensions in terms of social engineering on Facebook, as well as the source characteristics that influence Facebook users to judge an attacker as credible and therefore make them susceptible to becoming a victim. In this paper, we aim to test the findings of our previous work quantitatively using a role-play experimental method, and to examine to what extent those factors, which were explored in the previous work, affect user victimization. Moreover, in order to predict users' susceptibility to social engineering victimization based on their characteristics, we want to investigate whether there is any relationship between the effectiveness of those factors that influence Facebook users to judge an attacker as credible and users' demographics. This type of mixed methods design, which starts with a qualitative method followed by a quantitative method, is known as the sequential exploratory mixed method (Tashakkori and Teddlie 2003).

Literature Review and Theoretical Development

Susceptibility to Social Engineering

Several studies in information systems have investigated individuals' susceptibility to security victimization by studying employees' compliance with organizations' security policies. This has been done by relying on a number of theories and techniques, such as protection motivation theory (e.g., (Posey et al. 2013; Posey et al. 2014; Johnston et al. 2015)), electroencephalography (Vance et al. 2014), technology threat avoidance theory (Herath et al. 2014), and routine activity theory (Wang et al. 2015). There seems to be a general agreement that an individual's compliance with information security policies is associated with making accurate judgments regarding threat. Most of the research that has investigated human behaviors with regard to social engineering threat has been done on phishing e-mail, which is a type of social engineering attack but in a different context than SNSs. In those studies, the effectiveness of (false) source credibility has been repeatedly demonstrated in phishing victimization (e.g., (Dhamija et al. 2006; Luo et al. 2012; Sussman; Siegal 2003)). Moreover, there are only a few e-mail phishing studies (e.g., (Workman 2008; Parrish Jr et al. 2009; Kumaraguru et al. 2009; Kvedar et al. 2010; Sheng et al. 2010; Pattinson et al. 2012; Wright et al. 2014)) that have measured susceptibility to specific types of e-mail phishing attacks, or have studied the effectiveness of one or more phishing countermeasures in relation to some demographic factors. The difference between our study and those studies is that our focus is on social engineering in Facebook, and not in e-mail. Social engineering in Facebook involves several other techniques, such as posts, tags, applications, games, impersonation using fake profiles, and even interactive persuasion using chatting or messaging. Moreover, the focus of our study is on investigating how people judge attackers, and which source characteristics they base these judgments on, which have not been explored even in e-mail phishing studies. Recently, deception in SNSs have attracted many researchers. For example, there are several studies that have made contributions in regard to classifying the identity, mostly the gender, of the profiles' owners, (e.g., (Al Zamal et al. 2012; Liu and Ruths 2013; Rao et al. 2010; Pennacchiotti and Popescu 2011; Mislove et al. 2011; Alowibdi et al. 2014)). These studies generally used text-based characteristics as well as a set of features extracted from the accounts for classifying the users based on the profiles' content. Moreover, there are some studies that focused on detecting spamming in SNSs (e.g., (Chu et al. 2012; Huber et al. 2009; Thomas et al. 2013; Stringhini et al. 2010; Wang 2010; McCord and Chuah 2011; Castillo et al. 2011)), which used also profiles' content to detect if the account was automated or human. However, social engineers are usually human. Therefore, the benefits of the findings from previous studies remain limited in terms of social engineering.

Source Credibility

A social engineering attack 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 a request. In SNSs, obeying and accepting a message involves complying with a request, such as a request to click a link and the user clicks it, or a request to accept an offer and the user chooses to accept it. According to source credibility theory, people are more likely to obey and accept a message when the source presents itself as credible (Hovland et al. 1953). The theory is broken into the following three models: the factor, the functional, and the constructivist model. The aim of these models is to narrow the wide scope of the theory. That is, the factor model helps determine to what extent the receiver judges the source as credible. The functional model views credibility as the degree to which a source meets a receiver's needs. The constructivist model shows what the receiver does with the persuader's proposal or message. Source credibility research has its roots in persuasion. Aristotle divided the aspects of persuasion into three categories: ethos (credibility), pathos (emotion) and logos (logic). As emotion and logic indicate a person's emotional connection and means of reasoning to convince one of a particular argument, credibility refers to people believing who they trust (Burke 1966). For decades, marketers, advertisers, politicians, and researchers in human communication have investigated the effects of source characteristics on the beliefs, attitudes, or behaviors of the audience with regard to the contents of a message. A highly credible source is commonly found to be more persuasive than a low-credibility one (Hovland and Weiss 1951; Johnson and Izzett 1969; Kelman and Hovland 1953; Klebba and Unger 1983; Koslin et al. 1967; Pornpitakpan 2004).

Because of the many different operationalizations that appear in the literature, many definitions have been presented for source credibility. Due to the purpose of this research, which is exploring the source characteristics that influence Facebook users to judge an attacker as credible, we have adapted the definition of Ohanian 1990, where he defined source credibility as "a term commonly used to imply a communicator's positive characteristics that affect the receiver's acceptance of a message" (Ohanian 1990). Credibility is considered a perception (Tseng and Fogg 1999). It is a complex concept that is composed of other concepts called dimensions. In fact, many things can impact the perceived credibility of a source, depending on the type of that source, and the characteristics of the medium, channel, or environment (Metzger et al. 2003). Therefore, several dimensions of source credibility have been proposed such as intimacy, character, esteem, sociability, and clarity, depending on the type of the source and the type of the contexts (e.g., (Berlo et al. 1969; Markham 1968; Salwen 1987; Mosier and Ahlgren 1981; Corina 2006; Singletary 1976)). By looking at social engineering attacker, we can see that the type of the source is different and the type of context (Facebook) is also diffetrent than those studied before (Kane et al. 2014). Therefore, it was essential that, if we wish to study the credibility of a social engineering attacker in SNSs, a specific investigation has to be conducted specifically for that purpose.

Conceptualization

The a priori model and research hypotheses have been explored and developed in our previous works (Algarni et al. 2014a), and (Algarni et al. 2014b). This section will present an overall summary of the theoretical development and conceptualization. Source credibility theory, which was explained in the previous section, is the overarching theoretical framing of this study. While validating or violating source credibility dimensions in terms of social engineering on Facebook is a substantial contribution, our aim is not limited to this end. That is, we also want to link these dimensions to Facebook-based characteristics. Because no existing theory or model that can be applied to address the aim of the research, Creswell (2012) suggested using the grounded theory method to inductively build the targeted model.

> *Grounded theory is a good design to use when a theory is not available to explain the process. The literature may have models available, but they were developed and tested on samples and populations other than those of interest to the qualitative researcher. (Creswell 2012, p66).*

Grounded theory is a research method that seeks to develop a theory inductively that is grounded in data (Myers 1997). There has been increasing interest in the use of grounded theory in information systems research, due to its usefulness in developing theories within different and new contexts (Urquhart et al. 2010). The challenge of this topic is that the participants might claim that they are aware of deceptive practices and cannot be deceived. At best, they would admit that they do not know how they have been deceived. For this kind of challenge, Flick (2004) suggested using *triangulation*, which refers to the use of more than one method to investigate a research question. In our previous works, we used between-method triangulation, including observation and interviews (24 participants), and an open-ended questionnaire (72 participants), to explore the dimensions of source credibility in terms of social engineering attacks on Facebook. As represented in Figure 1, four potential dimensions of source credibility were found: perceived sincerity, perceived competence, perceived attraction, and perceived worthiness. Moreover, we found that there are 13 Facebook-based source characteristics that influence Facebook users to judge the attacker according to one of the credibility dimensions. That is, the source characteristics that have an impact on the perceived sincerity dimension are: 1) number of friends (the number of members the source is connected to), 2) common friends (the number of members that the source and the user are connected to in common), 3) number of posts that the source has made, 4) common beliefs (sharing a common religion with the user), and 5) the source's use of a real name (not using a nickname as an identifier). The source characteristics that have an impact on the perceived competence dimension are: 1) qualifications (educational level), 2) celebrity, and 3) wealth. The source characteristics that have an impact on the perceived attraction dimension are: 1) good looks and 2) good writing skills. The source characteristics that have an impact on the perceived worthiness dimension are: 1) authority (power over the user), 2) sexual compatibility with the user, and 3) reciprocity (the compliments, likes, and positive comments received from the source). In the following sections we present overall summary about those four dimensions based on our previous qualitative work and supportive theoretical evidence from literature.

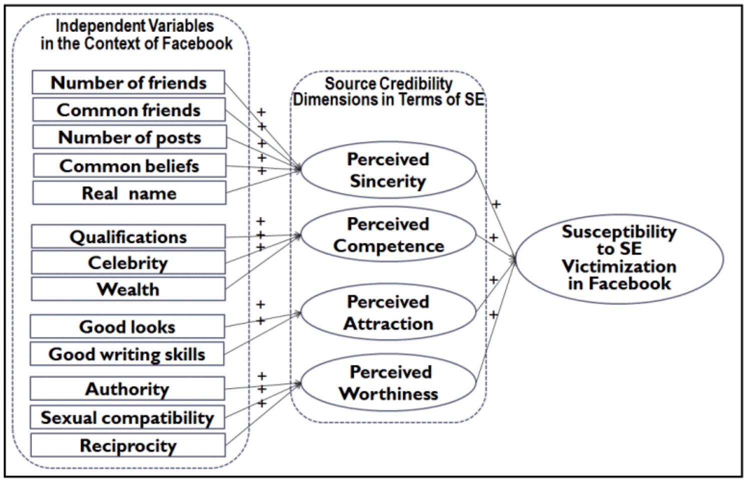

Figure 1. Source Credibility Dimensions in Terms of Social Engineering on Facebook.

Perceived Sincerity

Sincerity is the degree to which the message receiver perceives the source as honest and free from duplicity. Source characteristics related to sincerity were repeatedly mentioned in the interviews that were conducted in the qualitative phase. For instance, one of the interviewee reported *"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. Those factors are 1) number of friends (e.g., *"If that was the case, he wouldn't have only a few friends … The account was absolutely fake*"); 2) number of posts (e.g., "*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*"); 3) having a friend in common with the source (e.g., "*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*"); 4) sharing the same beliefs (e.g., "*having the same religion can make you sympathize with someone. I think it encourages you to help");* and 5) the use of a real name (e.g., "*I think they [those who use nicknames] are trying to hide their reality from others and there must be a reason for that*").

The role of perceived sincerity is explained in the literature by the factor model of *Source credibility theory,* which helps determine to what extent the receiver judges the source as credible. Perceived sincerity of a source makes the victim feel safe and therefore not perceive the threat. *Safety*, is the feeling of being protected from danger and risk. According to Pyszczynski et al. (1997), when people are threatened, they will alter their behavior depending on the number of risks they can accommodate. This modification is a psychological reaction that is determined by the seriousness of an attack and the amount of loss that they think will incur because of the occurrence of a hazard (Rosenstock 1974). This can explain how participants make judgment about sincerity of a source based on information available on the source profile such as number of friends, number of posts, using real name, and so on, which can give them perhaps some indications about the risk associated with such a source. The impact of number of friends and mutual friends can be explained further by the *Principle of social proof.* Social proof is doing what others do regardless of the importance or the correctness of that action (Lun et al. 2007). It is the influence of others on the behavior of someone. It can lead people to do things that might not be in their interest (Cialdini 2001). Social proof has been found to be one of the more powerful strategies in persuasion (Cialdini et al. 1999). The risk of this principle from the security perspective is that people behave according to the general attitude rather than what is secured. *Social judgment theory* can give an explanation about the impact of sharing the same belief on accepting a message. It suggests that people evaluate and judge the content of any message based on their anchors, or stance, on a particular topic or message. That is, people accept the message or reject it based on their cognitive map (Sherif and Hovland 1961). We therefore hypothesize the following:

Ha1: Users' susceptibility to social engineering victimization is positively related to the perceived sincerity of the source.

Hb1: The perceived sincerity of a source increases as the source's number of friends increases.

Hb2: The perceived sincerity of a source increases as the number of friends they have in common with the source increases.

Hb3: The perceived sincerity of a source increases as the number of the source's posts increases.

Hb4: The perceived sincerity of a source is positively related to sharing the same beliefs or religion with the source.

Hb5: The perceived sincerity of a source is positively related to the source's use of a real name.

Perceived Competence

The second dimension of source characteristics that influence Facebook users to judge others as credible is the source's competence or expertise. This concept represents the quality of being adequate and possessing a required skill or capacity. Three characteristics observed in the qualitative data reflect the dimension of competence: 1) qualifications (e.g., "*I think that the primary benefit of social networks is that they allow you to build a network of qualified and expert people in your field");* 2) celebrity (e.g., "*we always see them [*celebrities] *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*"); and 3) wealth (e.g., "*I have never thought that this guy is a scammer. From his photos you can tell that he is well educated, drives luxury cars, and lives in a beautiful home").*

The impact of perceived competence is strongly associated with trust in the literature. Trust has been studied in marketing in relation to persuasion, and it has been found that the characteristic of trusting people in advertisement is important in formulating marketing persuasion (Chen and Barnes 2007). Retailers utilize this weakness to persuade users that they have the endorsement of celebrities, high qualified, and wealthy people (Cialdini 2001). It has been shown through research that most people are drawn closer to individuals they are fond of and they end up developing trust for them (Seiter and Gass 2010). This explains why people tend to believe online professionals even if their expertise is not reflected in the profiles or sites that they operate. Trust has been studied in information systems as well, and it has been found that there is a strong relationship between trusting beliefs and trusting intentions (Vance et al. 2008). This, therefore, leads users to become vulnerable to the trustee sources in a situation of uncertainty (Vance et al. 2008). The impact of educational level on the perceived competence has been argued in the literature. For example, Crisci and Kassinove (1973) have studied the impact of ("Dr." versus "Mr.") on behavioural compliance, and the result of their study has shown significant effect of educational level on the perceived competence. Research shows that people tend to trust other people because they are experts, popular (such as celebrities), and wealthy (Hadnagy 2010; Mitnick and Simon 2001). Ekman (2007) explains that these characteristics can be used to influence some people to do anything in order to get affection from those who have them. Social engineers could pretend to be celebrities, wealthy, or high educated in order to trick users into maintaining ties with them (Hadnagy 2010), and hence the hypotheses:

Ha2: Users' susceptibility to social engineering victimization is positively related to the perceived competence of the source.
Hb6: The perceived competence of a source is positively related to the source's qualifications.
Hb7: The perceived competence of a source is positively related to the celebrity of the source.
Hb8: The perceived competence of a source is positively related to the wealth of the source.

Perceived Attraction

The dimension of attraction represents the feature or the quality that evokes interest and liking. Two characteristics observed in the qualitative data reflect the dimension of attractiveness: 1) good looks (e.g., "*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")*; and 2) good writing skills (e.g., "*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").*

The impact of attraction on accepting a message is associated with source likability in the literature. *Ben Franklin effect theory* states that when we like someone we are more willing to do him/her a favor (Jecker and Landy 1969). The reverse effect is also true. That is, when we do a person a favor, we tend to like them more as a result. It has been shown through research that people tend to communicate with other people because they are charming or attractive (Cialdini 2001; Ekman 2007). Several studies have been conducted in marketing research and the results of those studies concluded that communicators who have good looks are consistently liked more and have a positive impact on influencing others (Joseph 1982). The impact of writing skills on a message acceptance can be explained through the central route of *Elaboration likelihood model* (Petty and Cacioppo 1986). The central route uses message elaboration and can produce a positive attitude change and encourage the receiver to obey. Centrally routed messages include a wealth of information, rational arguments, and evidence to support a particular conclusion. If the argument of the message is strong, it will create a positive cognitive response in the minds of receivers while also positively aligning the receivers' beliefs with those views of the persuader. On the other hand, if the argument is weak, it will produce a negative cognitive response to the persuasive message, which in turn prevents an attitude change and causes the receiver not to obey. Recent study on blog reading behavior found that textual characteristics that appeal to the sentiment of the reader affect both reader attraction and retention (Singh et al. 2014). Therefore, we hypothesize the following:

Ha3: Users' susceptibility to social engineering victimization is positively related to the perceived attraction of the source.
Hb9: The perceived attraction of a source is positively related to the good looks of the source.
Hb10: The perceived attraction of a source is positively related to good writing by the source.

Perceived Worthiness

Perceived worthiness is the degree to which the source is perceived to be advantageous for the user to communicate with. In other words, it is the perceived benefit of the source, which inspires user's effort, respect, and care. The difference between worthiness and the previous dimensions is that it represents the potential benefit that the particular user can get from a source. Some participants of our qualitative work believe that the source must be worthy of their acceptance or response even if they believe the source is sincere, competence, or attractive (e.g., "*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. But if I don't care about him, I don't think that I'm willing to do that even if I believe that he is in need*"). The characteristics that were mentioned by participants in relation to the users' worthiness are 1) authority (e.g., *"When I see a post from my boss, I feel hesitant to leave it without commenting, sharing, or at least clicking the 'like' button.");* 2) sexual compatibility (e.g., "*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")*; and 3) reciprocity (e.g., *"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…generally speaking, I would try to make them happy and maintain a positive appearance for them").*

The role of perceived worthiness is explained in the literature by the functional model of *Source credibility theory,* which views credibility as the degree to which a source meets a receiver's needs (Hovland et al. 1953). *Politeness theory* also gives further explanation about the impact of perceived worthiness on accepting social engineering request. Politeness theory states that in response to any request, people maintain one of the two following faces: a positive-based face or a negative-based face (Brown and Levinson 1987). A positive-based face is one which reflects appreciating, or respecting. A negative-based face is one when there is no constraint in any way. In addition, the *Elaboration likelihood model* states that there are two routes or methods to influence others: the central route and the peripheral route (Petty and Cacioppo 1986). The peripheral route relies on a receiver's emotional involvement and thus persuade through more superficial means. The influences that were explained by participants in regards to authority, sexual compatibility, and reciprocity are all examples of peripheral cues or routes of *Elaboration likelihood model*. O'Connor and Seymour (2011) hold that these behaviors are determined partially by balancing the perceived benefits over losses in choosing to behave in a certain way. Social engineers pretend to be sexual match or important people in order to trick users into maintaining ties with them (Hadnagy 2010). Past research has provided a proof of the degree to which a person should give in to the wishes of a person in authority (Marusca 2014). Compliance is a behavior that makes a person keep conforming to those who have power over them. Therefore, the use of influence of authority to instill terror or panic causes people to submit to the "authorities" instructions. Social engineering thrives on those people who give in to fear and orders from influential people (Mitnick and Simon 2001). Reciprocity has also been a subject of corporate research. When people receive a favor from other people, they develop a feeling of discordance until favors are reciprocated (Hadnagy 2010). A person will have a penchant to give back in an equal measure whenever a chance presents itself. The degree to which people reciprocate compliment depends on the intrinsic value of that compliment assigned by the receiver. With continued reciprocity, a psychological commitment to adhere to decisions made in the past is cultivated, and it will sustain a consistent behavior that is attached to the decisions a person makes (O'Connor and Seymour 2011). Therefore, we hypothesize the following:

Ha4: Users' susceptibility to social engineering victimization is positively related to the perceived worthiness of the source.
Hb11: The perceived worthiness of a source is positively related to the authority of the source.
Hb12: The perceived worthiness of a source is positively related to their sexual compatibility with the source.
Hb13: The perceived worthiness of a source increases as the compliments, likes, and positive comments received from the source increase.

Method

Role-Play (Scenario-Based) Experiment

A type of experimental design called a role-play or scenario-based experiment was used to test the research hypotheses. In a role-play experiment, participants act out scripts, pictures, or examples based on real-life situations (Yardley-Matwiejczuk 1997). In the information security field, the role-play experiment method has been used in several phishing e-mail studies (e.g., (Dhamija et al. 2006; Downs et al. 2007; Furnell 2007; Pattinson et al. 2012; Sheng et al. 2010)) in which participants were presented with images of e-mails and then asked how they would respond if they received such an e-mail. We used a role-play experimental questionnaire in this study by presenting Facebook profiles that represent some source characteristics (manipulated variables) that we want to examine to the participants and asking them to rate every profile based on the information provided in those profiles. Every profile was presented along with a scenario that told the participants some information about the owner of the profile to enhance the participants' perception regarding the characteristics under study. To measure the items related to the credibility dimensions, we used a 10-point semantic differential scale, which is a type of rating scale designed to measure the connotative meaning of concepts (Garland 1990). This type of scale has been widely employed in past source credibility studies (e.g., (McCroskey et al. 1974; Gaziano and McGrath 1986; Burgoon 1976; Eisend 2006)).

To measure susceptibility to social engineering, we designed five social engineering requests (high risk actions) including tricks similar to those that have been used in real-life examples on Facebook such as Koobface, Zeus, Likejacking, Facebook Black, and Who-Viewed-Your-Profile attacks (Thomas and Nicol 2010; Baumhof and Shipp 2012; Baltazar et al. 2009; Clark 2013; Sadeghian et al. 2013). Two additional low risk requests were added to the role-play questionnaire in order to examine the impact of the manipulated variables on those low risk requests, and see whether their impact is different than their impact on high risk social engineering requests. For example, instead of providing the URL "http://www.facebooc.com/login/" (which is a clearly fake website and considered to be high risk), we used the URL "http://bit.ly/anyw" (which is not always an attacking attempt, and therefore considered to be low risk). As presented in Table 1, persuasive messages were added to those requests to encourage the participants to respond to (accept) the requests. Since we wanted to study the impact of the source who sent the trick and not the trick itself, we wrote the messages in a way that made the participants rely more on the source who wrote the message, for example, the messages included phrases such as "I have checked this myself," "I recommend that you download it," and so on. The participants were asked to indicate how they would respond to those requests if they were sent to them or posted by the owners of every profile shown to them. A 5-point Likert scale was used to measure the participants' consent intentions and behavior responses toward the social engineering requests, with a rating system of "Definitely yes" = 5, "Very probably yes" = 4, "Probably yes" = 3, "Very probably no" = 2, and "Definitely no" =1 (Albaum 1997). All items were developed and validated using a specific pilot study, as will be explained in scale development and testing section.

Social engineering tricks	Persuasive messages	Risk
Clickjacking through a video. The message (post) presents a video of "great white shark tears a captain apart in seconds" while the actual URL is: http://bit.ly/anyw Note: The mouse pointer is positioned on the video and the actual URL destination is displayed in the status bar as it would be if users prepared to click on the link on their own computer.	Most people can't watch this video for more than 25 seconds. It is really unbelievable!	Low
Clickjacking with executable file. The message offers a file that contains leaked government documents, while the actual extension is (.exe). The actual URL displayed in the status bar is: http://128.2.72.235/documents.jpg.exe	I'm deeply shocked. And, what's more, ashamed! Check out these recently leaked government documents.	High
Phishing through a post offering free cell phone minutes.	Yeah! Finally I found something for free. I received my minutes, and now you can too!	High
Downloading Who-Viewed-Your-Profile application/software.	It is safe and works very well. I have checked this myself. I recommend that you download it.	High
Spam or malware, by giving permission/access to the site before it allows the user to see a video.	Check this out. I watched it at least 20 times.	High
Phishing through a message from Facebook that threatens account suspension. The link in the message is written as: https://www.facebook.com/ while the actual URL displayed in the status bar is: http://www.facebooc.com/login/	Facebook started closing fake and duplicate accounts. Update your account soon. This is serious, I lost my old account :(	High
Clickjacking through a message containing a link that is written on the message as: http://www.youtube.com/watch?v=quali&fes while the actual URL displayed in the status bar is: http://bit.ly/anuyy	Take a look at this video that I found of (guess who?) – it's hilarious !	Low

Table 1. Social Engineering Requests/Tricks and Persuasive Messages.

Manipulated Variables Using a Fractional Factorial Design

Fractional factorial design (Gunst and Mason 2009) was used to design and manipulate the variables under study. This design allows researchers to minimize the number of experiments to utilize the participants' time and efforts better, and it provides a good way to calculate the effect of each source characteristic individually and interactively with others (Dey 1985). Based on the hypotheses that we wanted to examine, and using fractional factorial design, only 20 different Facebook profiles needed to be designed to examine the effectiveness of every variable of the 13 Facebook-based source characteristics (included in Hb1 to Hb13) that influence users to judge the attacker as credible, as represented in Table 2. Each profile represented one experiment, and each experiment was a combination of a low level, represented by (-), or high level, represented by (+), of the 13 source characteristics under study. Table 2 shows the characteristics for every profile that was shown to the participants in every experiment. For example, experiment 1 (Facebook profile 1) included a low number of friends, a high number of common friends, a high number of posts, a different belief (religion) than the participant, and a nickname as a profile identifier. For the rest of the source characteristics that were not related to the design of a particular experiment, such as good looking within experiment 1, we tried to make them as average as possible. To estimate the effect of one characteristic (manipulated variable), we calculated the variance and the effect size for its corresponding high level group, and compared it with its low level group. For example, if we wanted to calculate the effect of the variable "number of friends," we calculated the answers from experiments 1, 2, 3, and 4 as one component (representing the low level group), and compared it with the answers from experiments 5, 6, 7, and 8 as another component (high level group).

For some characteristics, such as sexual compatibility, we used different profiles representative of men and women. Part of the challenge in this stage was the difficulty of choosing people who were well known to the participants and who represented some of the experiments in the design well. The same difficulty was faced while preparing experiments 13 to 16, for which we needed to find posts that could be perceived as impressive or well written and other posts that could be perceived as badly written. Therefore, this task was done using two steps and two different groups of participants. The first group (44 women and 49 men) was asked to suggest or name up to three people for every experiment. This task was performed in a computer lab where the Internet was provided to the participants to help them choose, search, and take snapshots, and then e-mail their suggestions to the researcher. Then, the names of the people who were suggested more times by the first group were provided to the second group (46 women and 43 men) to rate every individual based on the characteristics under study. The same procedures were performed in regard to choosing the posts that represented low and high levels of writing skills.

	Number of Friends	Number of Common Friends	Number of Posts	Common Belief	Real Name	Qualification	Celebrity	Wealth	Good Looks	Good Writing Skills	Authority	Sexual Compatibility	Reciprocity
Profile/Experiment 1	-	+	+	-	-								
Profile/Experiment 2	-	-	-	-	+								
Profile/Experiment 3	-	+	-	+	-								
Profile/Experiment 4	-	-	+	+	+								
Profile/Experiment 5	+	-	+	-	-								
Profile/Experiment 6	+	+	-	-	+								
Profile/Experiment 7	+	-	-	+	-								
Profile/Experiment 8	+	+	+	+	+								
Profile/Experiment 9						+	+	+					
Profile/Experiment 10						-	-	+					
Profile/Experiment 11						+	-	-					
Profile/Experiment 12						-	+	-					
Profile/Experiment 13									+	+			
Profile/Experiment 14									-	-			
Profile/Experiment 15									-	+			
Profile/Experiment 16									+	-			
Profile/Experiment 17											+	+	+
Profile/Experiment 18											-	-	+
Profile/Experiment 19											+	-	-
Profile/Experiment 20											-	+	-

Table 2. The Design of the Experiments Based on Fractional Factorial Design.

Scale Development and Testing

As suggested by DeVellis (2012), we started with the representative items that have been used in the literature to measure the credibility. Second, we added other potential items that emerged from our previous work to the representative items that were drawn from the literature. The sample items were then assessed using the Delphi method. Delphi method is a structured, systematic, and interactive technique, which relies on a panel of experts. Those experts evaluate items under study in two or more rounds. After each round, experts are encouraged to refine their earlier items in light of the replies of other members of their panel. It is believed that during this process, the range of the items will decrease and the group will converge towards the correct items (Coates 1975; Dalkey and Helmer 1963). During the scale development and testing of this study, five information systems scholars were asked to evaluate the items of source credibility dimensions and make any necessary changes in order to eliminate repetitive items, non-user oriented items, and ambiguous items. The suggested measurement scale included differential semantic items that were given to the participants to rate the credibility dimensions of different Facebook profiles shown to them. In addition, social engineering requests that measure sucseptibility to social engineering have been tested using similar method. Three information security scholars were asked to evaluate the designed requests and make any required changes before we used them. The items of the credibility dimesnsions as well as the social engineering requests were then tested in a pilot study (before the present study), using a role-play experimental questionnaire. In total, 120 subjects participated in the pilot study by rating 2,400 Facebook profiles.

Approach and Procedures

After verifying the existence of the four dimensions in terms of the credibility of social engineering on Facebook and developing a valid measurement scale for measuring those dimensions and susceptibility to social engineering victimization, we conducted the present experiment using the validated measument scale that emerged from the pilot study. 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. Few organizations accepted the request. However, in order to avoid sample bias, ensure variation in demographics (e.g., gender, age, education level, security knowledge/awareness, and interest), and estimate nonresponse error, only three organizations, selectively, were recruited. The letter of invitation was distributed by email in a first and second round. Twitter and Facebook were also utilized as a third round (the invitation was posted on the three organizations' pages/accounts, and it was clearly mentioned that the participants had to be from these organizations). The first organization operates in the petroleum industry, the second organization operates in education, and the third organization operates in electricity production. All of the organizations are located in Saudi Arabia, where the characters (e.g., celebrities) used as experimental treatments were chosen from. In order to encourage more people to participate and to screen out those participants who were not paying attention to the questions, we offered to pay five US dollars to those participants that qualified by answering five qualifying questions, which could be answered correctly by a careful reading of the profiles' contents and the provided scenarios. In total, 377 participants completed the entire study, which constituted 7,540 profile observations for the required 20 experiments. The 20 profiles and their corresponding questions were displayed to the participants in random order. The overall response rate was 51% (43%, 63%, and 47% for the first, second, and third organizations, respectively). While 377 participants completed the entire study, only 37 participants started the experiment but did not complete them. These rates are considered to be average and similar to those reported by the majority of information systems research (Sivo et al. 2006). The participants who completed the study represented diversity in demographics, including both genders (around 60% male and 40% female), a variety of ages (around 30% from 18-25, 20% from 26-35, 25% from 36-45, and 25% over 45 years old), a variety of education levels (around 25% lower than a bachelor's degree, 35% bachelor's, 25% master's, and 15% PhD), and a variety of security knowledge levels (around 20% Level 1 (lowest), 40% Level 2, 20% Level 3, and 20% Level 4 (highest)). Around 65% of the participants responded after the first round of recruitment (using email), 20% after the second round (using email), and 15% after the third round (using Facebook and Twitter).

Although some researchers suggest asking participants about their demographics at the end of a questionnaire, we found that some demographics questions must be asked at the beginning of a questionnaire in order to examine the impact of some manipulated variables, such as sexual compatibility, celebrity, and common belief, which vary based on the participant's demographics. Therefore, participants were asked about their basic demographic information first, such as age and gender, and then specific profiles were displayed to them based on their demographics. The rest of the demographics were asked at the end of the questionnaire. Moreover, in similar role-play studies (e.g., (Sheng et al. 2010)) there was no difference between the impact of asking participants about their demographics at the beginning and the end of the questionnaire. All demographic information asked was basic and straightforward and used multiple choice answers, except the information related to the participant's security knowledge (security awareness level). For the security knowledge, we adapted four simple questions used by (Sheng et al. 2010), where the participants were asked to choose the best definition for four terms related to computer security: “cookie,” “phishing,” “spyware,” and “virus,” and they were given the same list of eight possible definitions to choose from for each. Questions and items have been presented in both English and Arabic language. 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, and they were approved by Human Research Ethics Committee at Queensland University of Technology. Key Survey 8.4 was used for the experimental questionnaire design and online data collection, and SPSS version 21.0 as well as AMOS version 22.0 were used in the data analysis.

Results

Factor Analysis and Data Screening

We started the analysis by assessing the requirements involved in structural equation modeling (SEM), which include: limited missing values; free of extreme outliers; not distorted significantly by the different opinions of specific groups; and the assumptions of normality and linearity upheld. Then, we computed the reliability coefficients of the scales using Cronbach’s alpha. Our previous work regarding scale development and testing, which was done prior to the present study using a pilot study, helped in eliminating problematic measurement items. As presented in Table 3, the overall reliability of Cronbach’s alpha value for the overall items used in the study was 0.94, and the Cronbach’s alpha values for perceived sincerity (6 items), perceived competence (6 items), perceived attraction (6 items), perceived worthiness (6 items), and susceptibility to social engineering (5 items) were 0.93, 0.96, 0.94, 0.94, and 0.90, respectively. After testing reliability using Cronbach’s alpha, the semantic differential data were submitted to the principal component factor analyses implemented in SPSS. The factor analysis revealed five factors (four for credibility dimensions and one for susceptibility to social engineering) with an eigenvalue of 1 or greater. Table 3 shows the overall factor and item properties.

Factor (Dimension) Properties	Items	Number of Observations	Loading	Mean	Standard Deviation	Standard Error
Name: Sincerity Cronbach’s alpha: 0.93 Eigenvalue: 4.88 Variance Explained: .16	Honest/Dishonest	7540	0.728	4.34	1.79	0.018
	Sincere/Insincere	7540	0.851	4.56	1.99	0.020
	Trustworthy/Not Trustworthy	7540	0.837	4.60	1.99	0.020
	Safe/Dangerous	7540	0.841	4.57	2.0	0.021
	Believable/Unbelievable	7540	0.850	4.58	2.0	0.021
	Real Account/Fake Account	7540	0.835	4.50	1.9	0.019
Name: Competence Cronbach’s alpha: 0.96 Eigenvalue: 5.31 Variance Explained: .18	Professional/Unprofessional	7540	0.872	4.45	2.12	0.024
	Competent/Incompetent	7540	0.843	4.50	2.11	0.024
	Qualified/Unqualified	7540	0.881	4.43	2.13	0.025
	Powerful/Powerless	7540	0.860	4.51	2.12	0.024
	Expert/Inexpert	7540	0.873	4.46	2.14	0.024
	Successful/Unsuccessful	7540	0.874	4.43	2.15	0.024
Name: Attraction Cronbach’s alpha: 0.94 Eigenvalue: 4.76 Variance Explained: .16	Attractive/Unattractive	7540	0.847	4.44	1.89	0.025
	Expressive/Inexpressive	7540	0.826	4.58	1.98	0.025
	Appealing/Unappealing	7540	0.774	4.81	1.93	0.024
	Interesting/Uninteresting	7540	0.817	4.64	1.95	0.024
	Cheerful/Gloomy	7540	0.803	4.57	1.94	0.024
	Exciting/Dull	7540	0.851	4.50	1.93	0.024
Name: Worthiness Cronbach’s alpha: 0.94 Eigenvalue: 4.78 Variance Explained: .16	Worthwhile/Worthless	7540	0.819	5.04	1.95	0.019
	Advantageous/Disadvantageous	7540	0.772	4.81	1.96	0.020
	Beneficial/Unbeneficial	7540	0.805	5.12	1.94	0.020
	Useful/Useless	7540	0.840	4.99	1.90	0.020
	Eligible/Not Eligible	7540	0.838	4.98	1.91	0.021
	Valuable/Invaluable	7540	0.807	5.02	1.98	0.020
Name: Susceptibility to Social Engineering Cronbach’s alpha: .90 Eigenvalue: 2.79 Variance Explained: .10	SE Request1	7540	0.654	2.71	0.68	0.007
	SE Request2	7540	0.670	2.72	0.69	0.007
	SE Request3	7540	0.658	2.70	0.69	0.008
	SE Request4	7540	0.665	2.70	0.68	0.007
	SE Request5	7540	0.660	2.72	0.68	0.007

Table 3. Dimensions and Item Properties.

Testing Hypotheses Ha1 to Ha4

Hypotheses Ha1 to Ha4 propose that there are positive relationships between susceptibility to social engineering victimization and the perceived sincerity, competence, attraction, and worthiness of the source. In other words, we wanted to examine the possibility of predicting susceptibility to social engineering victimization based on the perceived sincerity, competence, attraction, and worthiness of the source. For more validity and to gain more explanation about the impact of the factors involved in the hypotheses (Ha1 to Ha4), we ran hierarchical regression analyses using SPSS 21.0. We estimated four hierarchical regression analyses for four different models. The first model only contained perceived sincerity as a predictor of social engineering victimization. In the second to fourth models, we added one more independent factor each time to the previous model in a stepwise manner. The rationale for using this technique is to see whether the resulting model improves by including the four factors of perceived sincerity, competence, attraction, and worthiness as predictors. In other words, we will be able to see how much better the explanatory power becomes if a particular dimension is added or deleted (Tabachnick and Fidell 2001). However, linear regression requires some assumptions to be met, including the assumption of the reliability of the measurement, linearity, homoscedasticity, and normality of the error distribution (Osborne and Waters 2002). The reliability of measurement has been explained in the previous sections, and we showed that this assumption has been met. Further tests were conducted in regard to the linearity, homoscedasticity, and normality of the error distribution, and the results showed that our data met the acceptable levels regarding these issues. Table 4 shows the coefficients that resulted from the hierarchical linear regression analysis, and the four estimated model summaries.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics		R Square	Adjusted R Square	F Change	Sig. of F Change
		B	Std. Error	Beta			Tolerance	VIF				
1	(Constant)	1.778	.015		118.491	<.0001			.37	.37	742.7	<.0001
	Sincerity	.206	.003	.609	66.722	<.0001	1.000	1.000				
2	(Constant)	1.424	.014		99.932	<.0001			.54	.54	470.2	<.0001
	Sincerity	.156	.003	.461	56.333	<.0001	.891	1.123				
	Competence	.130	.002	.448	54.744	<.0001	.891	1.123				
3	(Constant)	1.241	.015		83.618	<.0001			.60	.60	162.9	<.0001
	Sincerity	.129	.003	.380	46.282	<.0001	.792	1.263				
	Competence	.114	.002	.392	49.087	<.0001	.840	1.191				
	Attraction	.083	.003	.243	29.474	<.0001	.786	1.273				
4	(Constant)	1.041	.015		67.593	<.0001			.64	.64	168.4	<.0001
	Sincerity	.140	.003	.412	52.751	<.0001	.779	1.284				
	Competence	.086	.002	.271	36.276	<.0001	.717	1.395				
	Attraction	.042	.003	.123	14.163	<.0001	.630	1.589				
	Worthiness	.093	.003	.295	31.061	<.0001	.623	1.604				

Table 4. Coefficient Results of the Hierarchical Linear Regression Analysis.

The results presented in Table 4, showed that every factor of perceived sincerity, competence, attraction, and worthiness significantly contributed to the prediction of susceptibility to social engineering victimization and the overall model fit gained significant improvement every time. That is, adding these factors step-by-step increased the R square of the regression models from 0.37 for estimated model 1 (which has perceived sincerity only as a predictor) to 0.64 for estimated model 4 (which considers perceived sincerity, competence, attraction, and worthiness as predictors). This increase happened with the changes in R square being significant in each step (F change = 742.7, $p < 0.01$ for model 1; F change = 500.0, $p < 0.01$ for model 2; F change = 156.3, $p < 0.01$ for model 3; and F change = 170.2, $p < 0.01$ for model 4). This provides more evidence that our proposed model (model 4 in Table 4) has more explanatory power. The coefficient results presented in Table 4 for the final model (model 4) show that all the correlation coefficients were significant at $p < 0.001$, and that perceived sincerity was the strongest predictor, with beta value = 0.412; then perceived worthiness, with beta value = .295; perceived competence, with beta value = .271; and perceived attraction, with beta value = .123. The results also showed a high percentage explained by the model, with $R^2 = 0.64$. We can see that these results are not identical, but very similar, to the values from AMOS 22.0, which is a normal and common occurrence in such statistical applications. Finally, the collinearity statistics were examined. Multi-collinearity is present when tolerance is close to 0 (< 0.01) or variance inflation factor (VIF) is high (> 10), in which case the beta and p coefficients may be unstable. The VIF and tolerance measures shown in Table 4 suggest that multi-collinearity is not an issue in our data. We can conclude that we have enough evidence to accept hypotheses Ha1 to Ha4.

Testing Hypotheses Hb1 to Hb13

To test these hypotheses we conducted t-tests to evaluate the differences between the participants' responses toward the credibility dimensions, for the profiles that contained low levels of the treatments (the variables under study) and compared them with the profiles that contained high levels of the treatments. We started by testing hypotheses Hb1 to Hb5, which propose that the perceived sincerity of a source increases, and as the source's number of friends, the number of friends the user has in common with the source, and the source's number of posts increase, and that the perceived sincerity of a source is positively related to sharing the same beliefs and the source's use of a real name. As explained earlier, our fractional factorial design contains eight experiments (profiles) for perceived sincerity: four contain a low level of the variable under study, and the other four contain a high level of the variable under study. For example, for the variable "number of friends" we conducted t-tests to measure the difference between the participants' responses toward perceived sincerity for experiments 1, 2, 3, and 4 (since they were given profiles that contained a low number of friends) and compared them with the participants' responses toward perceived sincerity for experiments 5, 6, 7, and 8 (since they were given profiles that contained a high number of friends). Cohen's distance (d) was also used along with the t-test comparisons, in order to present the differences between the groups in terms of standard deviation units (Cohen 1977). Table 5 presents the results of t-tests and effect size estimations for the hypotheses from Hb1 to Hb13.

Constructs (hypotheses)	Treatment Group	Cases (N)	Standard Deviation	Mean	T Value	P	Mean Difference	Cohen's d
Number of Friends (Hb1)	Low Level	1508	1.119257	4.0752	-33.493	<.0001	1.834	1.219
	High Level	1508	1.809194	5.9101				
Number of Common Friends (Hb2)	Low Level	1508	1.080642	4.3256	-22.464	<.0001	1.334	0.818
	High Level	1508	2.03764	5.6598				
Number of Posts (Hb3)	Low Level	1508	1.37236	4.3715	-20.69	<.0001	1.242	0.753
	High Level	1508	1.88538	5.6139				
Common Belief (Hb4)	Low Level	1508	1.28314	4.6149	-12.053	<.0001	0.755	0.439
	High Level	1508	2.06843	5.3705				
Real Name (Hb5)	Low Level	1508	0.77483	4.2234	-26.653	<.0001	1.538	0.970
	High Level	1508	2.10369	5.762				
Qualifications (Hb6)	Low Level	754	1.00983	3.3967	-23.577	<.0001	1.674	1.214
	High Level	754	1.66828	5.0711				
Celebrity (Hb7)	Low Level	754	1.03808	3.2069	-32.067	<.0001	2.054	1.651
	High Level	754	1.42001	5.2611				
Wealth (Hb8)	Low Level	754	1.04701	3.8464	-9.610	<.0001	0.775	0.494
	High Level	754	1.95180	4.6216				
Good Looks (Hb9)	Low Level	754	1.13137	3.0009	-29.902	<.0001	2.213	1.540
	High Level	754	1.68897	5.2146				
Good Writing Skills (Hb10)	Low Level	754	0.83095	3.8450	-5.682	<.0001	0.525	0.292
	High Level	754	2.3994	4.3705				
Authority (Hb11)	Low Level	754	0.60613	3.9812	-72.586	<.0001	3.775	3.738
	High Level	754	1.29313	7.7564				
Sexual Compatibility (Hb12)	Low Level	754	1.57132	5.3689	-9.321	<.0001	0.999	0.480
	High Level	754	2.49111	6.3687				
Reciprocity (Hb13)	Low Level	754	1.61952	5.3718	-9.264	<.0001	0.994	0.477
	High Level	754	2.46121	6.3658				

Table 5. T-Tests and Effect Sizes for Hypotheses Hb1-Hb13.

As presented in Table 5, the t-tests show significant effects of the treatments on the perception of sincerity, with (p value < 0.0001, t value = -33.4, and Cohen's d = 1.219) for the number of friends; (p value < 0.0001, t value = -22.4, and Cohen's d = 0.818) for the number of common friends; (p value < 0.0001, t value = -20.69, and Cohen's d = 0.753) for the number of posts; (p value < 0.0001, t value = -12.053, and Cohen's d = 0.439) for sharing a common belief; and (p value < 0.0001, t value = -26.653, and Cohen's d = 0.970) for using a real name. Similar techniques were used to test hypotheses Hb6 to Hb13, in which we conducted t-tests and used Cohen's d to measure the participant's responses toward perceived competence, perceived attraction, and perceived worthiness. As presented in Table 5, the t-tests show significant effects of the source's qualifications, celebrity, and wealth on influencing users to perceive the source as competent. The t-tests also show significant effects of the source's good looks and the source's good writing skills on influencing users to perceive the source as attractive. Similarly, t-test shows that the authority of the source, sexual compatibility with the source, and the reciprocity have significant effects on users' perceptions of worthiness. Therefore, we can conclude that we have enough evidence to accept hypotheses Hb1 to Hb13.

Demographics Analysis

Although we have examined the impact of the source's characteristics on the participants' perceptions toward the source credibility dimensions during the hypotheses testing, it would also be interesting to examine whether any of those characteristics have significantly different impacts on any particular demographic group. For this purpose, we ran a two-way ANOVA to examine whether there were any significant interactions between the effects of the source's characteristics (which are the treatments given to the participants) and the participants' demographic groups. Table 6 presents all the interactions that are significant at p < = 0.05, as well as the pairwise comparisons (measuring the difference between the differences, which occurred due to the treatments).

Interaction Specifications					Effect of the Treatment (Mean Difference) for These Demographic Group				
Interaction	**F**	**Sig**	**Observed Power**	**P. Eta Square**					
Number of Friends with User's Gender	109.7	<.0001	1.0	0.036	Female	Male			
					0.811	2.34			
Number of Common Friends with User's Educational Level	2.75	0.04	0.67	0.003	Lower than Bachelor	Bachelor	Masters	PhD or Doctorate	
					0.86	1.20	1.62	1.64	
Number of Posts with User's Educational Level	2.09	0.05	0.64	.002	Lower than Bachelor	Bachelor	Masters	PhD or Doctorate	
					0.89	1.17	1.41	1.55	
Using Real Name with User Gender	33.59	<.0001	1.0	0.011	Female	Male			
					2.20	1.20			
Qualifications with User's Gender	7.72	0.005	0.79	0.005	Female	Male			
					1.90	1.20			
Qualifications with User's Security Knowledge	7.15	<.0001	0.99	0.019	Lowest Level	Level 2	Level 3	Level 4	Highest Level
					1.74	1.71	1.52	1.17	0.39
Qualifications with User's Age	2.64	0.031	0.743	0.007	18-25 Years	26-35	36-45	46-55	56 and Over
					1.06	1.03	1.45	1.58	1.71
Celebrity with User's Age	3.32	0.01	0.84	0.009	18-25 Years	26-35	36-45	46-55	56 and Over
					2.29	1.87	1.91	1.53	1.39
Celebrity with User's Gender	10.8	0.001	0.90	0.008	Female	Male			
					2.26	1.62			
Wealth with User's Gender	53.8	<.0001	1.0	0.036	Female	Male			
					2.050	0.480			
Good Looks with User's Gender	8.75	0.003	0.84	0.006	Female	Male			
					2.60	1.95			
Authority with User's Educational Level	3.76	0.01	0.76	0.007	Lower than Bachelor	Bachelor	Masters	PhD or Doctorate	
					3.71	3.41	3.68	3.90	

Table 6. Significant Interactions Between Treatment Effects and User Demographics.

Although all hypothesized source characteristics were found to induce a significant influence on the users' judgments for all demographic groups, the results presented in Table 6 show that some source characteristics have even more impact on particular demographic groups. For example, we can see that the source's number of friends has a statistically significant interaction with the user's gender (F = 109, p < 0.0001). By running pairwise comparisons, we can see that the number of friends has more impact on males, with a mean difference = 2.34, compared to a mean difference = 0.811 for females. The partial eta square presented in the table shows the proportion of variance in the dependent variable that is explained by the independent variable, and the observed power shows that our sample size was adequate (Cohen 1977). Finally, all the post-hoc tests, which compared the groups presented in the table with each other, were statistically significant at p < 0.01.

Then, we examined the relationship between demographics and susceptibility to social engineering by measuring the participants' susceptibility to social engineering victimization in general, and regardless of the source's type of influence. This was done first by measuring the participants' responses to the five high risk social engineering requests. As presented in Table 7, a regression analysis shows that the participants' security knowledge significantly and linearly predicts their susceptibility to social engineering victimization (beta value = -0.10, p < 0.0001). An analysis of variance (ANOVA) comparing the security knowledge groups shows that the more security knowledge the participants have, the less susceptible they are (F(4, 7535) = 99.25, p < 0.0001). The results also show that gender has a significant effect on susceptibility to social engineering (beta value = -0.05, p < 0.0001), with a t-test showing that women are more susceptible than men (t(7538) = 10.423, p < 0.0001). In addition, the results show that the time elapsed since joining Facebook is a significant predictor of susceptibility to social engineering (beta value = -0.02, p = 0.001), and an ANOVA test shows that the less time elapsed, the more susceptible the user is (F(4,7535) = 10.59, p < .0001). Finally, the results show that age is a significant predictor of susceptibility to social engineering (beta value = -0.04, p < 0.0001), and the ANOVA tests show that young adults are more susceptible to social engineering (F(4,7535) = 15.06, p < .0001).

Regression Analysis			Variance Tests		Means				
Demographic	Standardized Coefficient	Sig	T or F Values	Sig					
Security knowledge	- .10	<.0001	F = 99.25	<0.0001	Lowest Level	Level 2	Level 3	Level 4	Highest Level
					2.89	2.76	2.74	2.69	2.40
Gender	- .05	<.0001	T = 10.42	<0.0001	Female		Male		
					2.81		2.66		
Time elapsed since joining Facebook	- .02	.001	F = 10.59	<0.0001	6 Months or Less	6 Months to 1 Year	1 to 2 Years	2 to 3 Years	More than 3 Years
					2.80	2.73	2.71	2.69	2.63
Age	- .04	<.0001	F = 15.06	<0.0001	18-25 Years	26-35	36-45	46-55	56 and Over
					2.81	2.70	2.68	2.69	2.66

Table 7. Regression Analysis for Demographic Groups and Group Differences.

Finally, we examined the participants' responses toward the two low risk requests. The rationale behind adding these requests and analyzing them was to examine to what extent participants rely on the source's characteristics when they respond to social engineering requests. The results showed that the participants were affected by the source's characteristics when they were encountered by high risk social engineering requests and low risk requests, with no significant difference. The results of the demographics analysis are interesting in a number of ways. First, they provide more validity in regard to the questions used to measure susceptibility to social engineering victimization. That is, the results showed that the requests used to measure social engineering mimic real life situations, where those tricks are more identifiable by people who are knowledgeable about security but not by normal users, including highly educated people in different study areas. Second, the results show that the majority of the participants in this study relied on the source's characteristics when they answered the experimental questionnaire, and therefore, the results give more validity that the arguments used in the messages have achieved the goal, which is studying the impact of the source characteristics. Third, although the security knowledgeable people were less willing to respond to social engineering requests, the results show that the source's characteristics still have influence on them to accept social engineering requests from attackers that look credible to them (since the beta value was only -0.10).

Structural Model and Fitting Assessment

Model fit assessment was performed on the model using AMOS (version 22.0) to confirm whether the collected data are an appropriate fit to the hypothesized model. The values of the correlations between Sincerity, Competence, Attraction, Worthiness, and Susceptibility to Social Engineering Victimization (SE_ Susceptibility) provided an indication of the discriminant validity, where all correlations were less than .55 between the independent constructs and less than .70 when both independent and dependent constructs were included. This validity refers to the extent to which a construct is distinct from other constructs (Hair et al. 2006). In addition, all the factor loadings were high and significant at the p < .01 level, suggesting convergent validity. This validity refers to the degree to which an item is related to the construct (Hair et al. 2006). The 13 Facebook-based characteristics are not included in the model since they were given directly as treatments, and therefore they were assessed using a t-test and an analysis of variance. We can see in Figure 2 that some values (e.g., beta values and model fit) are not identical, but very similar, to the results of SPSS, which is a normal and common occurrence in such statistical applications. In addition, assessments were done in regard to the goodness of fit. The resulted model appears to have a good fit, with the following values: minimum discrepancy (chi-square, χ^2) divided by the degrees of freedom (df) = 4.75; goodness of fit index (GFI) = .98; comparative fit index (CFI) = .99; incremental fit index (IFI) = .99; and root mean square error of approximation (RMSEA) = .022. These values satisfy the requirements suggested by structural equation modeling (Hair et al. 2006; Hooper et al. 2008).

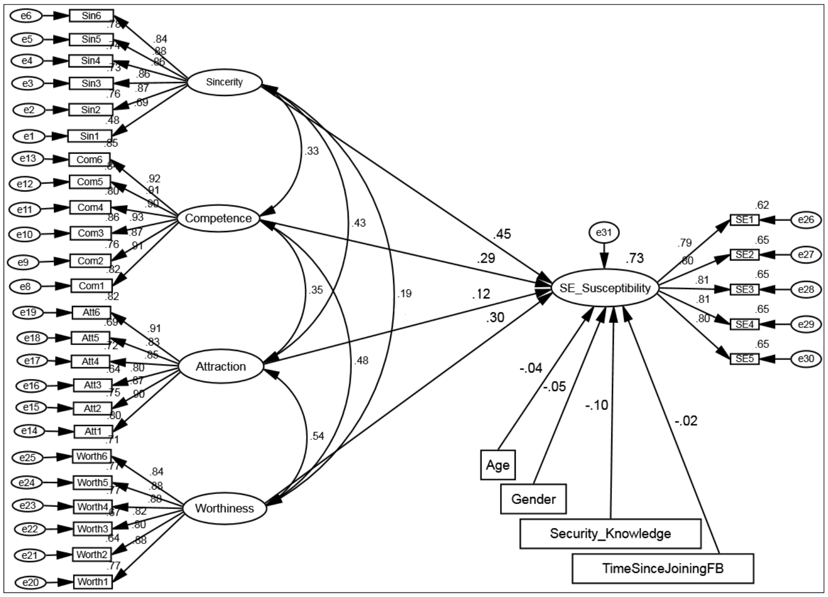

Figure 2: Model Fit Assessment, Using AMOS 22.0

Discussion and Conclusion

The results of this study have shown that every factor of the perceived sincerity, competence, attraction, and worthiness of a source are significant predictors of susceptibility to social engineering victimization, with a high percentage of the variance explained. Perceived sincerity was found to induce the most influence on users' judgment toward accepting or rejecting social engineering-based attacks on Facebook, then perceived worthiness, perceived competence, and perceived attraction. The results also explained which, and to which extent, source characteristics influence Facebook users to judge an attacker according to one of the source credibility dimensions. That is, the results have shown that the source characteristics that have a significant impact on perceived sincerity, ordered by the most effective influence, are 1) number of friends, 2) the source's use of a real name, 3) common friends, 4) number of posts, and 5) common beliefs. The source characteristics that have an impact on perceived competence, ordered by the most effective influence, are 1) celebrity, 2) qualifications (educational level), and 3) wealth. The source characteristics that have an impact on perceived attraction, ordered by the most effective influence, are 1) good looks and 2) good writing skills. The source characteristics that have an impact on perceived worthiness, ordered by the most effective influence, are 1) authority, 2) sexual compatibility, and 3) reciprocity. These characteristics render Facebook users susceptible to attackers, who can use fake profiles, accounts, pages, and identities to entrap victims.

Moreover, the results have shown that demographic groups differ in their perceptions and behaviors toward social engineering requests. To the best of our knowledge, no study has been dedicated to understanding which demographic variables correlate with falling victim to social engineering-based attacks in SNSs. However, there are some studies that have been done in regard to phishing e-mails, which usually use social engineering-based persuasion but in a different environment than SNSs. Those studies have indicated that there is a relationship between falling victim to phishing e-mails and demographic variables such as age, gender, and educational level. In this study, we investigated the relationship between falling victim to social engineering victimization in a new environment, Facebook, and we went further by investigating the relationship between demographic variables and different tricks that are used by attackers to influence users to become victims. The results have shown that people are different in their judgments and vulnerabilities, and therefore measuring susceptibility should be done by using the type of trick and not only whether the user became a victim or not, as has been done repeatedly in phishing e-mail studies.

The findings of the research must be viewed in light of the following limitations. First, due to the challenges of the ethical issues associated with running this experiment in the actual Facebook environment, permission issues from the owners of Facebook, and to conduct the study in accordance with the National Statement on Ethical Conduct in Research Involving Humans, we have used a role-play experiment. Using a role-play (scenario-based) experiment to measure users' behaviors may arguably differ from using an actual experiment. However, various studies have confirmed the degree of realism and involvement that can be achieved in role-playing studies (e.g., (Haney et al. 1973; Mixon 1972; O'Leary et al. 1970; Dhamija et al. 2006; Downs et al. 2007; Furnell 2007; Pattinson et al. 2012; Sheng et al. 2010)). Moreover, the several reliability and validity tests performed on the collected data of this study suggest that there is no reason to believe that the predictors described in this study should differ in their relationship to role-play behavior compared to real-world behavior. Second, while we have taken intensive steps to ensure the use of representative social engineering-based requests, we cannot guarantee that we have covered all types of tricks that can be used by attackers. In fact, social engineering is very broad, and it is sometimes difficult to classify a request as an attacking attempt or legitimate request (purely risky or purely safe). However, the focus of this study was on the characteristics of the source who sends the message, not the message's characteristics itself. In addition, with adequate consistency among the requests for all the experiments and enough variance between each experiment (treatment) and the others, validity for the requests used to measure social engineering susceptibility was achieved.

The overall results speak to the simplicity with which individuals can be deceived in SNSs, the theoretical reasons for why and how individuals fall victim to social engineering attacks, and the ways in which organizations' security defenses can be compromised through such deceptions. The findings have a number of important implications. First, identifying the links between the source's characteristics and the users' (as receivers) characteristics is a crucial step in data science, because it provides a theoretical foundation for developing effective applications and users' profiling mechanisms, which can automatically predict users' susceptibility to social engineering attacks based on their demographics. The results of this study are also crucial for organizational policy makers who aim to control insider threats based on theoretical knowledge. The findings of this study are also very useful for security education, training, and awareness (SETA) programs; and computer monitoring, which have been suggested as the best practices for deterring human-based information security incidents (D'Arcy et al. 2009). They can be very helpful as well for software engineers and SNS providers, because they point out that the lack of authentication of identities, photos, applications, and pages make SNSs dangerous weapons in the hands of scammers and social engineers who may take criminal advantage of users. The source characteristics that were found in this study are freely available for the attackers, they have a strong influence on users to fall victim to social engineering, and therefore they require urgent authentication solutions. SNS providers are encouraged to establish mechanisms that can help users make better judgments about the credibility of others. Feasibility studies could be conducted to see whether showing some real information about SNSs users, such as their locations, frequency of use, and multiple profile usage can reduce the risks associated with impersonation and identity theft in SNSs. Showing friendship requests that the user has received and that the user has sent can also help those who rely on the number of friends (as a reputation clue) when they make judgments about the credibility of a source. Applications that automatically friend others, create posts, and send messages to other users must be controlled. Phone numbers, formal e-mails, and other trusted mechanisms should be utilized to authenticate celebrities, authorities, public figures, and organizations' representatives. Finally, since we focused on the source's characteristics within the Facebook environment in this study, future research could focus on expanding the findings by utilizing more samples that are representative of various SNSs. Future research could also focus on investigating message characteristics and their impacts on SNSs users' susceptibility to social engineering victimization.

References

Albaum, G. 1997. "The Likert Scale Revisited," *Journal-Market Research Society (39:2),* pp. 331-348.

Algarni, A., Xu, Y., and Chan, T. 2014a. "Social Engineering in Social Networking Sites: The Art of Impersonation," in *Proceedings of the 2014 IEEE International Conference on Services Computing (SCC)*, Anchorage, Alaska, USA: IEEE Computer Society, pp. 797-804.

Algarni, A., Xu, Y., Chan, T., and Tian, Y.-C. 2013a. "Social Engineering in Social Networking Sites: Affect-Based Model," in *Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST),* IEEE Computer Society, pp. 508-515.

Algarni, A., Xu, Y., Chan, T., and Tian, Y.-C. 2013b. "Toward Understanding Social Engineering," in *Law & Practice: Critical Analysis and Legal Reasoning*, Kierkegaard, Sylvia (eds.), Copenhagen, Denmark: International Association of IT Lawyers, pp. 279-300.

Algarni, A., Xu, Y., Chan, T., and Tian, Y.-C. 2014b. "Social Engineering in Social Networking Sites: How Good Becomes Evil," in *Proceedings of the 18th Pacific Asia Conference on Information Systems (PACIS 2014)*, Chengdu, China: Association for Information Systems, Paper-271.

Alowibdi, J. S., Buy, U. A., Yu, P. S., and Stenneth, L. 2014. "Detecting Deception in Online Social Networks," in *Proceedings of 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM),* Beijing, China: IEEE, pp. 383-390.

Al Zamal, F., Liu, W., and Ruths, D. 2012. "Homophily and Latent Attribute Inference: Inferring Latent Attributes of Twitter Users from Neighbors," in *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media (ICWSM)*, Dublin, Ireland: Association for the Advancement of Artificial Intelligence, pp. 387-390

Baltazar, J., Costoya, J., and Flores, R. 2009. "The Real Face of Koobface: The Largest Web 2.0 Botnet Explained," *Trend Micro Research* (5:9), p. 10.

Baumhof, V., and Shipp, A. 2012. "Zeus P2p Advancements and Mitb Attack Vectors." *ThreatMetrix™ Labs Public Report,* San Jose, CA: ThreatMetrix Inc.

Berlo, D. K., Lemert, J. B., and Mertz, R. J. 1969. "Dimensions for Evaluating the Acceptability of Message Sources," *Public Opinion Quarterly* (33:4), pp. 563-576.

Braun, R., and Esswein, W. 2013. "Towards a Conceptualization of Corporate Risks in Online Social Networks: A Literature Based Overview of Risks," in the proceedings of the *17th IEEE International Enterprise Distributed Object Computing Conference (EDOC),* Vancouver, BC, Canada: IEEE Computer Society, pp. 267-274.

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

Brown, P., and Levinson, S. C. 1987. *Politeness: Some Universals in Language Usage*, Cambridge, United Kingdom: Cambridge University Press.

Burgoon, J. K. 1976. "The Ideal Source: A Reexamination of Source Credibility Measurement," *Communication Studies* (27:3), pp. 200-206.

Burke, K. 1966. *Language as Symbolic Action: Essays on Life, Literature, and Method*. Oakland, California: University of California Press.

Castillo, C., Mendoza, M., and Poblete, B. 2011. "Information Credibility on Twitter," in *Proceedings of the 20th International Conference on the World Wide Web*, New York, USA: ACM, pp. 675-684.

Chen, Y.-H., and Barnes, S. 2007. "Initial Trust and Online Buyer Behaviour," *Industrial Management & Data Systems* (107:1), pp. 21-36.

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.

Chu, Z., Gianvecchio, S., Wang, H., and Jajodia, S. 2012. "Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?" *IEEE Transactions on Dependable and Secure Computing* (9:6), pp. 811-824.

Cialdini, R. B. 2001. *Influence: Science and Practice (4th ed.),* Boston, USA: Allyn & Bacon.

Cialdini, R. B., Wosinska, W., Barrett, D. W., Butner, J., and Gornik-Durose, M. 1999. "Compliance with a Request in Two Cultures: The Differential Influence of Social Proof and Commitment/Consistency on Collectivists and Individualists," *Personality and Social Psychology Bulletin* (25:10), pp. 1242-1253.

Clark, K. 2013. "Five Notorious Facebook Attacks (Learn How to Protect Yourself)." *Social Media* Retrieved 2/3/2015, 2015, from http://www.hongkiat.com/blog/five-facebook-attacks/

Coates, J. F. 1975. "In Defense of Delphi:. A Review of Delphi Assessment, Expert Opinion, Forecasting, and Group Process by H. Sackman," *Technological Forecasting and Social Change* (7:2), pp. 193-194.

Cohen, J. 1977. *Statistical Power Analysis for the Behavioral Sciences*, New York, USA: Academic Press.

Corina, S. 2006. "Marketing Communication in Online Social Programs: Ohanian Model of Source Credibility," *Journal of Empirical Generalisations in Marketing* (1:1), pp. 778-784.

Couper, M. 2013. "Is the Sky Falling? New Technology, Changing Media, and the Future of Surveys," *Survey Research Methods* (7:3), pp. 145-156.

Creswell, J. W. 2012. *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, Thousand Oaks, California, USA: Sage Publications.

Crisci, R., and Kassinove, H. 1973. "Effect of Perceived Expertise, Strength of Advice, and Environmental Setting on Parental Compliance," *The Journal of Social Psychology* (89:2), pp. 245-250.

Dalkey, N., and Helmer, O. 1963. "An Experimental Application of the Delphi Method to the Use of Experts," *Management Science* (9:3), pp. 458-467.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

DeVellis, R. F. 2012. *Scale Development: Theory and Applications*. Thousand Oaks, California, USA: Sage Publications.

Dey, A. 1985. *Orthogonal Fractional Factorial Designs*. New York, USA: Wiley.

Dhamija, R., Tygar, J. D., and Hearst, M. 2006. "Why Phishing Works," in *Proceedings of the 2006 SIGCHI Conference on Human Factors in Computing Systems*, New York, USA: ACM, pp. 581-590.

Dimensional-Research. 2011. "The Risk of Social Engineering on Information Security: A Survey of IT Professionals," Technical Report, Long Beach, CA.

Downs, J. S., Holbrook, M., and Cranor, L. F. 2007. "Behavioral Response to Phishing Risk," in *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, New York, USA: ACM, pp. 37-44.

Eisend, M. 2006. "Source Credibility Dimensions in Marketing Communication—A Generalized Solution," *Journal of Empirical Generalizations in Marketing* (10:2), pp. 1-33.

Ekman, P. 2007. *Emotions Revealed: Recognizing Faces and Feelings to Improve Communication and Emotional Life*. New York, USA: Henry Holt and Company.

Fire, M., Goldschmidt, R., and Elovici, Y. 2014. "Online Social Networks: Threats and Solutions," *Communications Surveys & Tutorials, IEEE* (16:4), pp. 2019-2036.

Flick, U. 2004. "Triangulation in Qualitative Research," *A Companion to Qualitative Research*, London, United Kingdom: Sage Publications. pp. 178-183.

Furnell, S. 2007. "Phishing: Can We Spot the Signs?" *Computer Fraud & Security* (2007:3), pp. 10-15.

Garland, R. 1990. "A Comparison of Three Forms of the Semantic Differential," *Marketing Bulletin* (1:1), pp. 19-24.

Gaziano, C., and McGrath, K. 1986. "Measuring the Concept of Credibility," *Journalism Quarterly* (63:3), pp. 451-462.

Gunst, R. F., and Mason, R. L. 2009. "Fractional Factorial Design," *Wiley Interdisciplinary Reviews: Computational Statistics* (1:2), pp. 234-244.

Hadnagy, C. 2010. *Social Engineering: The Art of Human Hacking*. New York, USA: Wiley.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. 2006. *Multivariate Data Analysis*, Upper Saddle River, New Jersey, USA: Pearson Prentice Hall.

Haney, C., Banks, C., and Zimbardo, P. 1973. "Interpersonal Dynamics in a Simulated Prison," *International journal of criminology and penology* (1973:1), pp. 69-97

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., and Rao, H. R. 2014. "Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service," *Information Systems Journal* (24:1), pp. 61-84.

Hooper, D., Coughlan, J., and Mullen, M. 2008. "Structural Equation Modelling: Guidelines for Determining Model Fit," *Electronic Journal of Business Research Methods (6:1),* pp.*53 – 60.*

Hovland, C. I., Janis, I. L., and Kelley, H. H. 1953. *Communication and Persuasion; Psychological Studies of Opinion Change*. New Haven, CT, US: Yale University Press

Hovland, C. I., and Weiss, W. 1951. "The Influence of Source Credibility on Communication Effectiveness," *Public Opinion Quarterly* (15:4), pp. 635-650.

Huber, M., Kowalski, S., Nohlberg, M., and Tjoa, S. 2009. "Towards Automating Social Engineering Using Social Networking Sites," in the proceedings of 2009 *International Conference on Computational Science and Engineering,* Miami, USA : IEEE, pp. 117-124.

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

Jecker, J., and Landy, D. 1969. "Liking a Person as a Function of Doing Him a Favour," *Human Relations (22:4),* pp. 371-378.

Johnson, H. H., and Izzett, R. R. 1969. "Relationship between Authoritarianism and Attitude Change as a Function of Source Credibility and Type of Communication," *Journal of Personality and Social Psychology* (13:4), p. 317.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Joseph, W. B. 1982. "The Credibility of Physically Attractive Communicators: A Review," *Journal of Advertising* (11:3), pp. 15-24.

Kane, G. C., Alavi, M., Labianca, G. J., and Borgatti, S. P. 2014. "What's Different About Social Media Networks? A Framework and Research Agenda," *MIS Quarterly* (38:1), pp. 275-304

Kelman, H. C., and Hovland, C. I. 1953. "'Reinstatement' of the Communicator in Delayed Measurement of Opinion Change," *The Journal of Abnormal and Social Psychology* (48:3), p. 327.

Klebba, J. M., and Unger, L. S. 1983. "The Impact of Negative and Positive Information on Source Credibility in a Field Setting," *Advances in Consumer Research* (10:1), pp. 11-16.

Koslin, B. L., Stoops, J. W., and Loh, W. D. 1967. "Source Characteristics and Communication Discrepancy as Determinants of Attitude Change and Conformity," *Journal of Experimental Social Psychology* (3:3), pp. 230-242.

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," *in Proceedings of the 5th Symposium on Usable Privacy and Security*, New York, USA: ACM, pp. 1 - 12

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.

Toops, L. M. 2014. "7 Scary Findings from the 2014 Symantec Internet Security Threat Report," *Property & Casualty 360,* New York, USA: ALM Media Properties, LLC, from http://search.proquest.com/docview/1515280747?accountid=13380

Liu, W., and Ruths, D. 2013. "What's in a Name? Using First Names as Features for Gender Inference in Twitter," *In AAAI Spring Symposium: Analyzing Microtext*. Dublin, Ireland: Association for the Advancement of Artificial Intelligence, pp.10-16

Lun, J., Sinclair, S., Whitchurch, E. R., and Glenn, C. 2007. "(Why) Do I Think What You Think? Epistemic Social Tuning and Implicit Prejudice," *Journal of Personality and Social Psychology* (93:6), p. 957.

Luo, X. R., Zhang, W., Burd, S., and Seazzu, A. 2012. "Investigating Phishing Victimization with the Heuristic-Systematic Model: A Theoretical Framework and an Exploration," *Computers & Security (38:1),* pp. 28-38.

Markham, D. 1968. "The Dimensions of Source Credibility of Television Newscasters," *Journal of Communication* (18:1), pp. 57-64.

Marusca, L. 2014. "What Every Body Is Saying. An Ex-Fbi Agent's Guide to Speed-Reading People." *Journal of Media Research (7:3),* Cluj-Napoca: Accent Publisher, pp. 89-90

McCord, M., and Chuah, M. 2011. "Spam Detection on Twitter Using Traditional Classifiers," in *Autonomic and Trusted Computing*, Berlin, Heidelberg: Springer, pp. 175-186.

McCroskey, J. C., Holdridge, W., and Toomb, J. K. 1974. "An Instrument for Measuring the Source Credibility of Basic Speech Communication Instructors," *Communication Education* (23:1), pp. 26-33.

Metzger, M. J., Flanagin, A. J., Eyal, K., Lemus, D. R., and McCann, R. M. 2003. "Credibility for the 21st Century: Integrating Perspectives on Source, Message, and Media Credibility in the Contemporary Media Environment," *Communication Yearbook* (27), pp. 293-336.

Mislove, A., Lehmann, S., Ahn, Y.-Y., Onnela, J.-P., and Rosenquist, J. N. 2011. "Understanding the Demographics of Twitter Users," in Proceedings of the *Fifth International AAAI Conference on Weblogs and Social Media*, Barcelona, Spain: Association for the Advancement of Artificial Intelligence, pp.1-4.

Mitnick, K. D., and Simon, W. L. 2001. *The Art of Deception: Controlling the Human Element of Security*. New York, USA: Wiley.

Mixon, D. 1972. "Instead of Deception," *Journal for the Theory of Social Behaviour* (2:2), pp. 145-178.

Mosier, N. R., and Ahlgren, A. 1981. "Credibility of Precision Journalism," *Journalism & Mass Communication Quarterly* (58:3), pp. 375-518.

Myers, M. D. 1997. "Qualitative Research in Information Systems," *Management Information Systems Quarterly* (21:2), pp. 241-242.

Nagy, J., and Pecho, P. 2009. "Social Networks Security," in *Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies*, Athens, Glyfada: IEEE, pp. 321-325.

Nohlberg, M. 2009. "Why Humans Are the Weakest Link," in *Social and Human Elements of Information Security: Emerging Trends and Countermeasures, Gupta, M. and Sharman, R.* (eds.)*,* Hershey, USA*:* IGI Global, pp. 15-26.

O'Connor, J., and Seymour, J. 2011. *Introducing Nlp: Psychological Skills for Understanding and Influencing People*. San Francisco, USA. Conari Press.

Ohanian, R. 1990. "Construction and Validation of a Scale to Measure Celebrity Endorsers' Perceived Expertise, Trustworthiness, and Attractiveness," *Journal of Advertising* (19:3), pp. 39-52.

O'Leary, C. J., Willis, F. N., and Tomich, E. 1970. "Conformity under Deceptive and Non-Deceptive Techniques," *The Sociological Quarterly* (11:1), pp. 87-93.

Osborne, J., and Waters, E. 2002. "Four Assumptions of Multiple Regression That Researchers Should Always Test," *Practical Assessment, Research & Evaluation* (8:2), pp. 1-9.

Parrish Jr, J. L., Bailey, J. L., and Courtney, J. F. 2009. “A Personality Based Model for Determining Susceptibility to Phishing Attacks,” in *Janet Bailey*, Little Rock, USA: University of Arkansas, pp 285-296

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.

Pennacchiotti, M., and Popescu, A.-M. 2011. "A Machine Learning Approach to Twitter User Classification," in Proceedings of the *Fifth International AAAI Conference on Weblogs and Social Media*, Barcelona, Spain: Association for the Advancement of Artificial Intelligence, pp. 281-288.

Petty, R. E., and Cacioppo, J. T. 1986. "The Elaboration Likelihood Model of Persuasion," in *Communication and Persuasion*, Richard E. Petty and John T. Cacioppo (eds.), New York, USA: Springer, pp. 1-24.

Pornpitakpan, C. 2004. "The Persuasiveness of Source Credibility: A Critical Review of Five Decades' Evidence," *Journal of Applied Social Psychology* (34:2), pp. 243-281.

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., and Courtney, J. 2013. "Insiders’ Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189-1210.

Posey, C., Roberts, T. L., Lowry, P. B., and Hightower, R. T. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns between Information Security Professionals and Ordinary Organizational Insiders," *Information & Management* (51:5), pp. 551-567.

Pyszczynski, T., Greenberg, J., and Solomon, S. 1997. "Why Do We Need What We Need? A Terror Management Perspective on the Roots of Human Social Motivation," *Psychological Inquiry* (8:1), pp. 1-20.

Rao, D., Yarowsky, D., Shreevats, A., and Gupta, M. 2010. "Classifying Latent User Attributes in Twitter," in *Proceedings of the 2nd International Workshop on Search and Mining User-Generated Contents*, Toronto , Canada, pp. 37-44.

Rosenstock, I. M. 1974. "Historical Origins of the Health Belief Model," *Health Education & Behavior* (2:4), pp. 328-335.

Sadeghian, A., Zamani, M., and Shanmugam, B. 2013. "Security Threats in Online Social Networks," in the Proceedings of the 2013 *International Conference on Informatics and Creative Multimedia (ICICM)*: Kuala Lumpur, Malaysia: IEEE, pp. 254-258.

Salwen, M. B. 1987. "Credibility of Newspaper Opinion Polls: Source, Source Intent and Precision," *Journalism & Mass Communication Quarterly* (64:4), pp. 813-819.

Seiter, R., and Gass, J. 2010. *Persuasion, Social Influence, and Compliance Gaining*. Boston, USA: Allyn & Bacon.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. 2010. "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," in *Proceedings of the 2010 SIGCHI Conference on Human Factors in Computing Systems*, New York, USA: ACM, pp. 373-382.

Sherif, M., and Hovland, C. I. 1961. *Social Judgment: Assimilation and Contrast Effects in Communication and Attitude Change*. Oxford, England: Yale University Press.

Singh, P. V., Sahoo, N., and Mukhopadhyay, T. 2014. "How to Attract and Retain Readers in Enterprise Blogging?" *Information Systems Research* (25:1), pp. 35-52.

Singletary, M. W. 1976. "Components of Credibility of a Favorable News Source," *Journalism & Mass Communication Quarterly* (53:2), pp. 316-319.

Sivo, S. A., Saunders, C., Chang, Q., and Jiang, J. J. 2006. "How Low Should You Go? Low Response Rates and the Validity of Inference in IS Questionnaire Research," *Journal of the Association for Information Systems* (7:6), pp. 351-414.

Stringhini, G., Kruegel, C., and Vigna, G. 2010. "Detecting Spammers on Social Networks," in *Proceedings of the 26th Annual Computer Security Applications Conference*, Austin, USA: ACM, pp. 1-9.

Sussman, S. W., and Siegal, W. S. 2003. "Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption," *Information Systems Research* (14:1), pp. 47-65.

Tabachnick, B. G., and Fidell, L. S. 2001. *Using Multivariate Statistics (4th ed.).* Boston, Mass, USA: Allyn and Bacon.

Tashakkori, A., and Teddlie, C. 2003. *Handbook of Mixed Methods in Social & Behavioral Research*. Thousand Oaks, California, USA: Sage Publications.

Thomas, K., and Nicol, D. M. 2010. "The Koobface Botnet and the Rise of Social Malware," *in Proceedings of the 5th International Conference on Malicious and Unwanted Software (MALWARE),* Nancy Lorraine, France: IEEE, pp. 63-70.

Thomas, K., McCoy, D., Grier, C., Kolcz, A., and Paxson, V. 2013. "Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse," in *Proceedings of the 22nd Annual USENIX Security Symposium (Usenix Sec 2013),* Washington DC, USA: Citeseer, pp. 195-210.

Thornburgh, T. 2004. "Social Engineering: The Dark Art," in *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, New York, USA: ACM, pp. 133-135.

Tseng, S., and Fogg, B. 1999. "Credibility and Computing Technology," *Communications of the ACM* (42:5), pp. 39-44.

Urquhart, C., Lehmann, H., and Myers, M. D. 2010. "Putting the 'Theory' Back into Grounded Theory: Guidelines for Grounded Theory Studies in Information Systems," *Information Systems Journal* (20:4), pp. 357-381.

Vance, A., Anderson, B. B., Kirwan, C. B., and Eargle, D. 2014. "Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG)," *Journal of the Association for Information Systems* (15:10), pp. 679-722.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D. W. 2008. "Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture," *Journal of Management Information Systems* (24:4), pp. 73-100.

Wang, A. H. 2010. "Don't Follow Me: Spam Detection in Twitter," *in the Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT),* Athens, Greece: IEEE, pp. 1-10.

Wang, J., Gupta, M., and Raj, R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *Management Information Systems Quarterly* (39:1), pp. 91-112.

West, R., Mayhorn, C., Hardee, J., and Mendel, J. 2009. "The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions," *Social and Human Elements of Information Security: Emerging Trends and Countermeasures, Gupta, M. and Sharman, R.* (eds.), Hershey, USA*:* IGI Global, pp. 43-60

Workman, M. 2007. "Gaining Access with Social Engineering: An Empirical Study of the Threat," *Information Systems Security* (16:6), pp. 315-331.

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.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., and Marett, K. 2014. "Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," *Information Systems Research* (25:2), pp. 385-400.

Yardley-Matwiejczuk, K. M. 1997. *Role Play: Theory and Practice*. London, United Kingdom: Sage Publications.