information

Article

What Message Characteristics Make Social Engineering Successful on Facebook: The Role of Central Route, Peripheral Route, and Perceived Risk

Abdullah Algarni

Information Technology Division, Institute of Public Administration, Riyadh 11141, Saudi Arabia; algarniaa@ipa.edu.sa

Received: 14 February 2019; Accepted: 10 June 2019; Published: 13 June 2019

Abstract: Past research suggests that the human ability to detect social engineering deception is very limited, and it is even more limited in the virtual environment of social networking sites (SNS) such as Facebook. At the organizational level, research suggests that social engineers could succeed even among those organizations that identify themselves as being aware of social engineering techniques. This may be partly due to the complexity of human behaviors in failing to recognize social engineering tricks in SNSs. Due to the vital role that persuasion and perception play on users' decision to accept or reject social engineering tricks, this paper aims to investigate the impact of message characteristics on users' susceptibility to social engineering victimization on Facebook. In doing so, we investigate the role of the central route of persuasion, peripheral route of persuasion, and perceived risk on susceptibility to social engineering on Facebook. In addition, we investigate the mediation effects between the explored factors, and whether there is any relationship between the effectiveness of them and users' demographics.

Keywords: social engineering; deception; argument quality; persuasion; Facebook; Elaboration Likelihood Model

1. Introduction

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 [1–3]. Research indicates that people perform poorly in detecting social engineering attacks [4,5]. At the organizational level, research suggests that social engineers could succeed even among those organizations that identify themselves as being aware of social engineering techniques [6]. Several researchers have investigated and highlighted the risks associated with social engineering in SNSs (e.g., References [7–13]). These studies have suggested that SNSs are the most common source of social engineering threats nowadays. 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 [14].

The risk of social engineering attacks in SNSs is associated with how difficult it is for users to make accurate judgments and decision regarding deception in the virtual environment of SNSs. The heuristic-systematic mode [15–17] and Elaboration Likelihood Model (ELM) [18–20] have shown that persuasion relies on three main factors: Source characteristics, message (content) characteristics, and target (recipient) characteristics. In terms of social engineering in SNSs, Algarni et al. [21–23] have investigated the impact of source characteristics on users' susceptibility to social engineering victimization on Facebook. However, the impact of message characteristics on users' susceptibility to social engineering victimization on Facebook is still to be explored, which we attempt to achieve in this study.

A social engineering trick (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. For decades, marketers, advertisers, politicians, and researchers in human communication have investigated the effects of message characteristics on the beliefs, attitudes, or behaviors of the audience. Message characteristics are commonly found to yield favorable cognitive and affective responses to the message [24–30].

In this study, we examine the impact of message characteristics on users' susceptibility to social engineering from two angles: Information processing and risk perception. For the information processing, we rely on the Elaboration Likelihood Model (ELM). ELM proposes two distinct routes for information processing: A central route and a peripheral route [20]. The risk perception serves as additional sources of influence that may offset the favorable propensity changes from the central route and the peripheral route. Therefore, the central route, the peripheral route, and the risk perception are simultaneously examined in this study, in order to have a fuller picture of the impact of message characteristics on users' susceptibility to social engineering. The theoretical base chosen for this research, and the rationale and justification for this choice, are explained in more detail in Section 3.

The contribution of this study is twofold. First, we explore the message characteristics that influence the success of a social engineering trick in SNSs, using Facebook as a context. Second, we investigate the interaction effects between message characteristics and recipient characteristics (demographics). That is, we investigate whether there is any relationship between the effectiveness of the explored message characteristics and users' demographics. Predicting users' vulnerabilities based on their demographics represents a substantial practical contribution expected from this study's findings.

2. Context and Motivation

2.1. *Social Engineering in SNSs*

In the online environment, such as SNSs, susceptibility is the risk of falling victim to an attack performed through techniques such as phishing, spying, snooping or impersonation. Susceptibility to social engineering can be defined as the extent to which a user would fall victim to social engineering trick. Victimization in information security refers to the breach, damage, disabling, or obstruction of an information system (including the user) that prevents the system from ensuring its availability, integrity, authentication, confidentiality, and non-repudiation [31]. Most of the research that has investigated human behaviors regarding social engineering threat has been done on phishing e-mail, which is a type of social engineering attack but in a different context to SNSs. Some e-mail phishing studies (e.g., References [6,32–37]) 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 on Facebook, and not using e-mail. Social engineering on Facebook involves several other techniques, such as posts, tags, applications, games, impersonation using fake profiles, and even interactive persuasion using chatting or messaging [38]. Moreover, the focus of our study is on investigating how people judge social engineering tricks (attempts), and which message characteristics they base these judgments on, which have not been explored even in e-mail phishing studies.

Recently, the topic of social engineering in SNSs has attracted many researchers. For example, one research track that has tried to provide solutions to the social engineering issue involves spam detection (e.g., References [39–45]). Another research track involves the detection of bot-operated accounts. Its solutions aim to detect if a profile is operated by a human or a computer (bot) (e.g., References [39–43,45,46]). Another research track tried to classify the identity (usually the gender) of SNS profile owners (e.g., References [47–51]). Although these studies are valuable, social engineering still succeeds despite all the available technical methods. This is because the proposed methods focus on the weakness of the technology, not the weakness of the users. No social engineering-based attack can succeed unless the users themselves accept, succumb, and perform the requested action which harms them and benefits the attackers.

2.2. Choosing Facebook as a Context

Facebook was chosen as a context for the present study in particular for multiple reasons. The most obvious reason is that Facebook is the most ubiquitous SNS, with a user base that far exceeds other SNSs. At the time of writing, Facebook is the biggest social networking service based on global reach and total number of active users. The second reason for choosing Facebook as the setting for this research was that Facebook is a less specialized platform [52]. For example, LinkedIn is mostly used by professionals, Snapchat is used by those concerned with privacy, Instagram is mostly a photo-sharing platform, and Twitter is mostly a microblogging tool. Facebook has a publicly open structure, looser behavioral norms, and plenty of tools and features that members use to leave cues for each other [53]. This made Facebook the perfect setting for studying the impact of message characteristics on users' perceptions, judgments, decision, and susceptibility to social engineering victimization in SNSs.

3. Theoretical Framing and Pre-Study

3.1. Theoretical Base

ELM [20] is the main theoretical basis of this study. ELM is one of the often used dual-process theories demonstrated in prior psychology research, which have examined the role of influence in shaping human perception and behavior. We take the perspective of the ELM to understand how social engineering might explore human vulnerabilities. We consider that the underlying influence process in social engineering (via cues in the message) and the recipient's information process can be directly related to ELM. The flow of social engineering attack initiates at the moment a deceptive message reaches the target victim. As the recipient examines the persuasive arguments and the heuristic cues conveyed, he or she may be influenced or persuaded to give out valuable information or perform an action that benefits the attacker, and therefore fall victim to the social engineering attack.

ELM theory states that there are two routes or methods to influence others: The central route and the peripheral route. The central route uses argument quality, and it can produce a positive attitude change and encourage the receiver to obey. The peripheral route is the likely result of low elaboration and relies on a receiver's emotional involvement and thus persuades the receiver through more superficial means such as liking, scarcity, and social proof. As we aim to investigate the message characteristics that influence the success of social engineering trick on Facebook, we need to address the two parts that have been indicated in ELM: The content of the message (the wealth of information, rational arguments, and evidence to support a particular conclusion) and the superficial means of the message (the features, tools and resources that can be seen within, under, or around a particular message on Facebook, such as likes, comments, photos, and others).

In addition, past research suggests that there is a strong relationship between information processing and risk perception (e.g., References [54,55]). That is, information systems research suggests that SNSs users are skeptical about SNSs as a secure channel and they worry about the potential risks from attacks, losing private information, and losing monetary information [56]. In the context of social engineering in SNSs, such perceived risks are even more salient since the recipients are requested to give out personal information or perform an action in a virtual environment. SNSs involve more uncertainty and risk compared to traditional communication channels. Therefore, SNS users' risk perception serves as additional sources of influence; and they may even offset the favorable propensity changes from argument quality or peripheral cues. A user who is persuaded by a social engineering trick may not necessarily submit his or her sensitive information in SNSs, in case he or she perceives high levels of risk. Consequently, we argue that, in addition to the influences from central and peripheral routes, perceived risk may have an impact on the recipient's propensity.

Although it is expected that the perceived risk may have a negative impact on the recipient's propensity to fall victim to social engineering (e.g., release personal information or perform a requested action), the extent to which the perceived risk impacts social engineering victimization is compared with argument quality and peripheral route. More importantly, it is interesting to investigate whether there is a relationship (e.g., mediation effect) between the superficial means (peripheral cues) of a message on Facebook and perceived risk. Attackers may exploit these superficial means as counter-risk approaches to reduce the perceived risks by the potential victims. Therefore, we attempt to explore the impact of message characteristics on users' susceptibility to social engineering victimization through investigating the role of the central route of persuasion, peripheral route of persuasion, and perceived risk on susceptibility to social engineering victimization.

3.2. Central Route of Persuasion (Argument Quality)

The central route of the Elaboration Likelihood Model (ELM) uses argument quality, and it can produce a positive attitude change and encourage the receiver to obey. The central route occurs when the recipient is motivated and able to think about the content of the message (elaboration is high). 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, and the information is complete, it will create a positive cognitive response in the mind of the receiver such as evaluation, recall, and critical judgment. On the other hand, if the argument is weak or the information is incomplete, it will produce a negative cognitive response to the persuasive message, which in turn prevents an attitude change.

While argument quality is commonly investigated in prior literature in several contexts such as marketing, advertisement, tourism, and information systems (e.g., References [24–30,57,58]), the operationalization and conceptualization of argument quality seem to be inconsistent among previous studies. However, for the purpose of exploring the message characteristics that influence Facebook users to accept social engineering request (trick), the present study defines argument quality as the extent to which received information can persuade a person to believe something or to perform an action [59–61].

Argument quality research has its roots in persuasion. The aspects of persuasion are divided into three categories: Ethos (credibility), pathos (emotion), and logos (logic) [62]. 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 whom they trust. Some researchers suggest that argument quality is composed of other concepts called dimensions [60]. Although argument quality has been measured from different angles in previous studies (e.g., References [59,63–66]) there seems to be a general agreement that these measurements are to assess either the information (e.g., information completeness, consistency, accuracy, adequacy, relevance, timeliness, and comprehensiveness) or the persuasion (e.g., persuasion strength, valence, and convince). These two dimensions also found to be valid in the case of examining the influence of online reviews on decision-making (e.g., References [26,60]). Therefore, we argue in this study that argument quality is a multidimensional concept, with two dimensions: The perceived informativeness and the perceived persuasiveness. We refer to perceived informativeness as users' perceptions regarding the quality of the information embedded in the message [60,67], while perceived persuasiveness represents the users' perceptions regarding the strength of persuasiveness embedded in the message [60,61]. Although the extent to which these dimensions apply to new and emerging SNS platforms is unclear, there is a reason to believe that high perceived informativeness and high perceived persuasiveness will have a positive effect on Facebook users' susceptibility to social engineering victimization. We therefore hypothesize the following:

H1: Perceived informativeness of a message positively affects susceptibility to social engineering victimization.

H2: Perceived persuasiveness of a message positively affects susceptibility to social engineering victimization.

3.3. Perceived Risk

Perceived risk refers to a person's perception of uncertainty about the safety of undertaking an action or activity [26]. Every person has a specific belief about the risk associated with any behavior he/she exhibits. This belief can be different from person to person, even with regard to the same action. Rosenstock [68] introduced a relationship between behavior and perceived risk through the Health Belief Model (HBM). This theory suggests that the probability of performing a risky action is determined by the perceived threat of taking that action, perceived susceptibility to the threat, perceived severity of the threat if it has already happened, and perceived benefits of taking that action. Protection Motivation Theory (PMT) also proposes that individuals protect themselves based on the perceived severity of a threatening event, perceived vulnerability (probability of the occurrence of that threat), efficacy of the recommended preventive action or behavior, and perceived self-efficacy [69]. Aldoory et al. [70] went further, stating that the problems of performing a risky action have been associated with the HBM and the situational theory of publics [71]. The latter suggests that a population can be classified depending on the way it behaves, that is, whether it is active or passive. The psychological issues concerned with this theory include: (1) The extent of activity in the behavior, (2) familiarization with problems, and (3) knowledge of constraints [72].

Zimbardo [73] explains that the level of familiarization with problems is different in different people; some believe that a predicament is more relevant to them, while others are not concerned with the same affliction. The extent of activity in this behavior varies depending on the feelings a person attaches to a predicament and the amount of loss that may be incurred in the case that an attack occurs [74]. The knowledge of constraints shows the degree to which people consider their mannerisms to be restrained by issues that are uncontrollable. According to Pyszczynski et al. [75], 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 be incurred due to a hazard. Perceived risk repeatedly negatively affects behavior intention (e.g., [26,76–78]). Because social engineering tricks are directly tied to several threats, perceived risk is an inherent attribute of accepting and responding to social engineering tricks. Based on this reasoning, we hypothesize:

H3: Perceived risk has a negative effect on susceptibility to social engineering victimization.

3.4. Peripheral Route of Persuasion

As indicated earlier, ELM states that there are two routes or methods to influence others: The central route and the peripheral route [20]. While the central route is the likely result of high elaboration and relies on argument quality, the peripheral route is the likely result of low elaboration, and relies on a receiver's emotional involvement and thus persuades the receiver through more superficial means such as liking, scarcity, and social proof.

ELM theory explains that perception of the recipient of the persuasion plays a vital role in accepting or rejection of a request in a message. This perception can be impacted by the characteristics of the medium, channel, or environment [79,80]. By looking at social engineering tricks and attempts on Facebook, we can see that the purpose of persuasion is different, and the type of context (Facebook) is also different than those studied before [81]. Therefore, it was important that, if we wish to study the impact of message characteristics on susceptibility to social engineering victimization on Facebook, we take into consideration the peripheral cues, which ELM describes as superficial means. The peripheral cues (superficial means) are the features, tools, and resources that can be seen within, under, or around a particular message on Facebook, such as likes, comments, and photos.

In order to explore the peripheral cues (superficial means) that might have an influence on Facebook users' perception and therefore decision to accept or reject social engineering trick, a pre-study using a focus group method was conducted [82]. Focus group is a qualitative research technique, which involves a group discussion guided by a trained leader. It has been found to be very useful in exploring people's pensions and experiences regarding emerging technology-driven phenomena [83], and to explore not only what people think but how they think and why they think that way. Two focus groups have been conducted. The first focus group includes 12 participants and the second focus group includes 9 participants. Any Facebook user who logs in to his/her account at least 4 times a week was eligible to participate. Invitations have been sent through some Facebook pages whose members are local residents. The invitation consisted of an invitation letter, a study information sheet, and a consent form. Participants with different demographic variables were selected to ensure that the sample represents a potentially high degree of variation and to increase the likelihood of identifying all possible factors under investigation. Both focus groups were conducted by the main researcher in a convenient room, where computers are available and connected to the Internet, for those participants who wish to observe Facebook during the discussion, so that they remember all possible characteristics under investigation.

Participants were asked to identify all possible message characteristics that might have an influence on their decision to believe or accept a message on Facebook. The discussions were audio recorded and the recordings transcribed verbatim. Since our interest is the message characteristics, any characteristic that is related to the source (user or page), such as user photo or user number of friends, has been discarded. Similarly, since our interest is the peripheral cues (superficial means), any characteristic that can be classified as central route persuasion has been discarded. The message characteristics that resulted from those focus groups and can be classified as peripheral cues included spelling, grammar, message length, supportive picture, supportive video, number of likes, number of comments, emoji (emoticons or smiley faces), and well-organization (properly-structured). While there was a general agreement between participants on some of these characteristics (e.g., spelling, grammar, message length, supportive picture, supportive video, number of likes), some other characteristics have only little agreement. However, we decided to include all of them in our experiment, and make our final conclusion regarding the significance of their effects based on statistical analysis, and hence the hypotheses:

H4: Correct spelling positively affects susceptibility to social engineering victimization.

H5: Correct grammar positively affects susceptibility to social engineering victimization.

H6: Susceptibility to social engineering victimization increases as the message length increases.

H7: Having supporting picture in a message positively affects susceptibility to social engineering victimization.

H8: Having supporting video in a message positively affects susceptibility to social engineering victimization.

H9: Susceptibility to social engineering victimization increases as the number of likes of a message increases.

H10: Susceptibility to social engineering victimization increases as the number of comments of a message increases.

H11: Having expressive emoji (emoticons or smiley faces) positively affects susceptibility to social engineering victimization.

H12: Susceptibility to social engineering victimization is positively related to a well-organized (properly-structured) message.

3.5. Interaction between Central Route Dimentions, Perceived Risk, and Peripheral Cues

As mentioned in Section 2.2, argument quality is a complex concept that is composed of other concepts called dimensions. Argument quality dimensions and risk are perceptions. Therefore, many factors can impact the perceived argument quality (e.g., perceived informativeness and perceived persuasiveness) and the perceived risk of a message, depending on the characteristics of the medium, the channel or the environment [80]. A review of extant literature shows that human perception towards a message has been studied in different contexts to different entities including human, media, technology, and information. These studies found that human perception towards a message on the internet is strongly impacted by superficial means (peripheral cues) [80]. Research showed that SNSs present new challenges for people to make judgment towards the argument quality, and the risk of a message that is posted in SNSs. The greatest challenge is that SNSs have provided access to an unprecedented amount of information that is freely available for the public. The information in SNSs also is not subject to the same degree of filtering through professional gatekeepers such as in news or trusted websites, and as a result, this information may be more prone to being incomplete, inaccurate, or unsecured.

One consequence of these challenges is the accompanying issue of finding the information that meets one's needs from among the enhanced amount of information that is posted in SNSs. The time that a user spends on reading every content is short compared with other websites, and it is based on a fast evaluation that relies mostly on peripheral cues. There are several studies (e.g., References [84–86]) that have investigated the factors that SNS users use when they make such an evaluation, and there seems to be a general agreement on the impact of peripheral cues, such as message length, interactivity (e.g., number of comments and likes), and message organization, on users' perception towards the argument quality, and the risk of a message. Although the extent to which the peripheral cues, which have been identified in Section 3.4, apply to social engineering on the Facebook platform is unclear, there is a reason to believe their effect on users' perception towards argument quality dimensions and risk. Examining the existence of these effects is conducted in Section 4.4 through examining interactions (e.g., mediations and moderations).

4. Method

4.1. Experimental Design

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 [87]. In the information security field, the role-play experiment method has been used in several phishing e-mail studies (e.g., References [34,35,88–90]) in which participants were presented with images of e-mails and then asked how they would respond if they received such an e-mail.

This study followed the same procedures. That is, we used a role-play experimental questionnaire in this study by presenting Facebook messages (posts) that represent some message characteristics (manipulated variables included in hypotheses H4–H12) to the participants and asking them to rate every message based on the information and argument (content) provided in those messages, and their intention to respond, with regards to the requested action (how would they respond to it).

To measure susceptibility to social engineering, we designed five social engineering requests, as presented in Table 1, 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 [91–95]). Persuasive messages were added to those requests to encourage the participants to respond to (accept) the requests. The persuasive messages have been designed with respect to the manipulated variables under study, included in hypotheses H4–H12 (the design of the experiments is explained in details in the next section). A random request of the five designed social engineering requests was presented, and the participants were asked to indicate how they would respond to this request if they see it posted, or if is sent 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 [96]. All items were developed and validated using a specific pilot study, as will be explained in scale development and testing section. Table 1 shows the specifications of the social engineering items that were used in the role-play experiment, and Appendix A presents an example of the designed messages.

Table 1. Social engineering requests/tricks.

	Social Engineering Tricks
1	**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
2	**Phishing** through a post offering free cell phone minutes.
3	**Downloading** Who-Viewed-Your-Profile application/software.
4	**Spam or malware**, by giving permission/access to the site before it allows the user to see a video.
5	**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/

4.2. Using Fractional Factorial Design

Fractional factorial design [97] 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 message characteristic individually and interactively with others [98]. Minitab 17.0 was used to suggest the experiments needed for this study. Minitab is a software application that states which main effects and interactions are confounded with an alias structure. Based on the hypotheses that we wanted to examine, and using fractional factorial design, only 16 different messages needed to be designed to examine the effectiveness of every variable of the 9 Facebook-based message characteristics (included in H4–H12), as represented in Table 2. Each message represented one experiment, and each experiment was a combination of a low level, represented by (−), or high level, represented by (+), of the 9 message characteristics under study. Table 2 shows the characteristics for every message that was shown to the participants in every experiment. For example, experiment 6 included a message with no spelling mistakes (high level), several grammar mistakes (low level), was relatively long (high level), had no picture (low level), had no video (low level), had a high number of likes (high level), had only two comments (low level), had a high number of emoji (high level), and was well-organized (high level). To estimate the effect of one characteristic (manipulated variable), we calculated the mean 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 "message length," we calculated the answers from experiments 1, 2, 3, 4, 9, 10, 11, and 12 as one component (representing the low level group), and compared it with the answers from experiments 5, 6, 7, 8, 13, 14, 15, and 16 as another component (high level group). This comparison is done through conducting an analysis of variance (ANOVA) and Eta-squared effect size, as will be explained in the results section.

Table 2. The design of the experiments based on fractional factorial design. Number of levels for each factor = 2, number of factors = 9, number of required experiments = 16, and resolution = 3 [97].

Treatments	Spelling	Grammar	Message Length	Supportive Picture	Supportive Video	Number of Likes	Number of Comments	Emoji	Well-Organization
Message/Experiment 1	−	−	−	−	−	−	−	−	+
Message/Experiment 2	+	−	−	−	+	−	+	+	−
Message/Experiment 3	−	+	−	−	+	+	−	+	−
Message/Experiment 4	+	+	−	−	−	+	+	−	+
Message/Experiment 5	−	−	+	−	+	+	+	−	−
Message/Experiment 6	+	−	+	−	−	+	−	+	+
Message/Experiment 7	−	+	+	−	−	−	+	+	+
Message/Experiment 8	+	+	+	−	+	−	−	−	−
Message/Experiment 9	−	−	−	+	−	+	+	+	−
Message/Experiment 10	+	−	−	+	+	+	−	−	+
Message/Experiment 11	−	+	−	+	+	−	+	−	+
Message/Experiment 12	+	+	−	+	−	−	−	+	−
Message/Experiment 13	−	−	+	+	+	−	−	+	+
Message/Experiment 14	+	−	+	+	−	−	+	−	−
Message/Experiment 15	−	+	+	+	−	+	−	−	−
Message/Experiment 16	+	+	+	+	+	+	+	+	+

To enhance the validity of the designed experiments, all messages have been designed and then tested regarding their corresponding manipulated variables using a group of participants. That is, a group of 16 participants (7 women and 9 men) was asked to rate every message based on the characteristics under study. This step has been conducted more than once for some characteristics (e.g., well-organization) until enough and suitable variance has been observed between the low and the high levels.

4.3. Measurement

As suggested by DeVellis [99], we started with the representative items that have been used in the literature to measure the factors under study (the perceived informativeness, the perceived persuasiveness, and the perceived risk). That is, we adapted previously validated items in the literature for perceived informativeness (e.g., References [60,67,100]), for perceived persuasiveness [59–61], and for the perceived risk [26,77,78,101]. Second, we slightly modified some of the wording of these items to fit the present research context. 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 [102,103]. During the scale development and testing of this study, four information systems scholars were asked to evaluate the items and make any necessary changes in order to eliminate repetitive items, non-user-oriented items, and ambiguous items.

In addition, social engineering requests that measure susceptibility to social engineering have been tested using a 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 perceived informativeness, perceived persuasiveness, perceived risk, and social engineering requests were then tested in a pilot study (before the present study), using a role-play experimental questionnaire. In total, 32 subjects participated in the pilot study by rating 512 messages (16 messages by every participant). The analysis of the pilot study has verified, initially, the existence of the two dimensions of the argument quality, and valid scales for measuring these dimensions as well as perceived risk. However, for more validly and reliability, we did not fully rely on the pilot study and we have tested them again in the present study, as explained in the next section.

4.4. Sample and Procedures

After verifying the existence of the two dimensions of the argument quality (perceived informativeness, perceived persuasiveness), and valid scales for measuring these dimensions as well as perceived risk, we conducted the present study using the validated measurement scales 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. From those who accepted the request, two organizations were recruited selectively, in order to avoid sample bias, ensure variation in the demographics (e.g., gender, age, education, security knowledge/awareness, and interest) and be able to estimate the non-response error. The letter of invitation was distributed by email for two rounds. The first organization operates in the education industry (located in Saudi Arabia), while the second organization operates in the telecommunication industry (located in the United Arab Emirates). In order to encourage more people to participate and to screen out those participants who were not paying attention to the questions, we offered a pizza voucher (equivalent to around 6 US dollars) to those participants that qualified by answering four qualifying questions, which could be answered correctly by a careful reading of the messages contents and questions. In total, 267 participants completed the entire study, which constituted 4272 message observations for the required designed 16 experiments (messages). The 16 experiments (messages) and their corresponding questions were displayed to the participants in random order. The overall response rate was 41% (45%

for the first organization, and 37% for the second organization). While 267 participants completed the entire study, 28 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 [104]. The participants who completed the study represented diversity in demographics, as shown in Table 3. Around 65% of the participants responded after the first round of recruitment, and around 35% after the second round.

Table 3. Demographics of the participants.

Variable	N (=267)	Percentage
Organization		
First organization	142	54%
Second Organization	125	46%
Gender		
Male	166	62%
Female	101	38%
Age		
From 18–25	80	30%
From 26–35	53	20%
From 36–45	72	27%
Over 45 years old	62	23%
Education Level		
Lower than a Bachelor's degree	66	25%
Bachelor's	96	36%
Master's	64	24%
PhD	41	15%
Security Knowledge Levels		
Level 1 (lowest)	53	20%
Level 2	99	37%
Level 3	67	25%
Level 4	48	18%
Round of Recruitment		
First round	174	65%
Second round	95	35%

The demographics information was asked at 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. [35] and Algarni et al. [23], 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. To control for random error and other issues, such as the confounding of the order of presentation and task (the order effects that can confound experiment results), we used the highly suggested strategy, which is known as counterbalancing. In counterbalancing, half of the subjects should have been given the low level of the treatment first, and the other half of the subjects should have been given the high level first. 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 Institute of Public Administration. 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.

5. Results

5.1. 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. Table 4 shows the overall factor and item properties.

Table 4. Dimensions and item properties.

Factor	Items	Number of Observations	Loading	Mean	Standard Deviation	Standard Error
Name: Perceived informativeness Cronbach's alpha: 0.91 Eigenvalue: 3.38 Variance Explained: 0.18	This message provided relevant information about the (document, application, offer, …)	4272	0.778	4.36	1.79	0.019
	This message provided complete information about the …	4272	0.881	4.46	1.98	0.020
	This message provided accurate information about the …	4272	0.837	4.62	1.97	0.021
	This message provided adequate information about the …	4272	0.846	4.67	2.1	0.021
Name: Perceived persuasiveness Cronbach's alpha: 0.93 Eigenvalue: 5.41 Variance Explained: 0.19	The argument of this message was convincing	4272	0.872	4.45	2.12	0.024
	The arguments of this message were persuasive	4272	0.853	4.50	2.1	0.023
	The arguments of this message were strong	4272	0.871	4.44	2.12	0.025
	The arguments of this message were good	4272	0.862	4.54	2.0	0.023
Name: Perceived risk Cronbach's alpha: 0.89 Eigenvalue: 4.86 Variance Explained: 0.15	How risky do you feel it would be to make a decision based on the message provided?	4272	0.847	4.45	1.89	0.025
	How risky do you feel it would be to accept and [download the document, download the application, etc.] based on the provided message?	4272	0.816	4.58	1.98	0.024
	How safe do you feel it would be to consent and [download the document, download the application, etc.] based on the provided message? [reversed]	4272	0.704	4.71	1.83	0.022

As presented in Table 4, the overall reliability of Cronbach's alpha value for the overall items used in the study was 0.91, and the Cronbach's alpha values for perceived informativeness (4 items), perceived persuasiveness (4 items), and perceived risk (3 items) were 0.91, 0.93, and 0.89, respectively. After testing reliability using Cronbach's alpha, the semantic differential data was submitted to the principal component factor analyses implemented in SPSS. The factor analysis revealed two dimensions for argument quality, and one factor for perceived risk with an eigenvalue greater than one.

5.2. *Hypotheses Testing*

Different and multiple statistical techniques were used to test our proposed hypotheses. First, we used linear regression analysis to test the hypotheses from H1–H3. Second, ANOVA and effect size estimations were used to test the hypotheses from H4–H12. Justifications, procedures, and other details of those tests will be explained in the following sections.

5.2.1. Testing Hypotheses H1–H3

Hypotheses H1–H3 propose that there are positive relationships between susceptibility to social engineering victimization and the perceived informativeness, perceived persuasiveness, and perceived risk. In other words, we wanted to examine the possibility of predicting susceptibility to social engineering victimization based on the perceived informativeness, perceived persuasiveness, and perceived risk. For more validity and to gain more explanation about the impact of the factors involved in the hypotheses (H1–H3), we ran step-wise regression analyses using SPSS 21.0. We estimated three step-wise regression models. The first model only contained perceived informativeness as a predictor of social engineering victimization. In the second to third 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 three factors of perceived informativeness, perceived persuasiveness, and perceived risk 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 [105].

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 [106]. The reliability of measurement has been explained in the previous sections, and we showed that this assumption has been met. Further tests were conducted regarding the linearity, homoscedasticity, and normality of the error distribution, and the results showed that our data met the acceptable levels regarding these issues. Table 5 shows the coefficients that resulted from the step-wise regression analysis, and the three estimated model summaries.

Table 5. Results of the step-wise regression analysis.

Model		Standardized Coefficients	t	Sig.	R Square	Adjusted R Square	F Change	Sig. of F Change
		Beta						
1	(Constant)		111.1	<0.0001	0.31	0.31	641.9	<0.0001
	Perceived informativeness	0.59	61.12	<0.0001				
2	(Constant)		97.73	<0.0001	0.42	0.42	469.2	<0.0001
	Perceived informativeness	0.41	46.32	<0.0001				
	Perceived persuasiveness	0.37	44.44	<0.0001				
3	(Constant)		73.19	<0.0001	0.46	0.46	212.8	<0.0001
	Perceived informativeness	0.36	41.2	<0.0001				
	Perceived persuasiveness	0.27	29.08	<0.0001				
	Perceived risk	0.29	33.73	<0.0001				

The results presented in Table 5 showed that every factor of perceived informativeness, perceived persuasiveness, and perceived risk 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 0.31 for estimated model 1 (which has perceived informativeness only as a predictor) to 0.46 for estimated model 3 (which considers perceived informativeness, perceived persuasiveness, and perceived risk as predictors). This increase happened with the changes in R square being significant in each step (F change = 641.9, $p < 0.0001$ for model 1; F change = 469.2, $p < 0.0001$ for model 2; and F change = 212.8, $p < 0.0001$ for model 3). This provides more evidence that our proposed model has more explanatory power. The coefficient results presented in Table 5 for the final model (model 3) show that all the correlation coefficients were significant at $p < 0.0001$, and that perceived informativeness was the strongest predictor, with beta value = 0.36; then perceived risk, with beta value = 0.29, then perceived persuasiveness, with beta value = 0.27. The results also showed a relatively high percentage explained by the model, with $R^2 = 0.46$. Therefore, we can conclude that we have enough evidence to accept hypotheses H1–H3.

5.2.2. Testing Hypotheses H4–H12

Hypotheses H4–H12 represent the message characteristics (peripheral cues), which were given to the participants as experimental treatments, and therefore they will be assessed using analysis of variance (ANOVA) and Eta-squared effect size. That is, ANOVA tests were conducted to evaluate the differences between the participants' responses toward susceptibility to social engineering, in the experiments (manipulated messages) that contained low levels of treatments, and in the messages experiments (manipulated messages) that contained high levels of treatments.

There are two options to perform this analysis: Using multiple comparisons on factor main effects, or using multiple comparisons among all factorial means of interest. Researchers (e.g., Reference [107]) indicate that multiple comparisons on factor main effects (factor means) are used if the main effects are significant and interactions are not significant. Therefore, we started our analysis by testing the interactions between the dependent variables (the 9-variable corresponding to the hypotheses H4–H12) and we found them statistically not significant. Therefore, the condition of using multiple comparisons on factor main effects is met. This step is important to avoid any multiple comparisons issue, such as a type 1 error.

As explained in Sections 3.1 and 3.2, the participants were asked to indicate how they would respond to the requests presented to them, based on A 5-point Likert scale. The A 5-point Likert scale was used to measure the participants' consent intentions and behavioral responses toward the social engineering requests (which represents susceptibility to social engineering), with a rating system of "Definitely yes" = 5, "Very probably yes" = 4, "Probably yes" = 3, "Very probably no" = 2, and "Definitely no" = 1. In addition, the fractional factorial design contained 16 experiments (manipulated messages). Eight of them contained a low level of the variable under study, and the other eight contained a high level of the variable under study.

For example, for the variable "Supportive picture", ANOVA tests were conducted to measure the difference between the participants' responses on susceptibility to social engineering victimization in Experiments 1, 2, 3, 4, 5, 6, 7, and 8 (as one group, since they were given messages that contained a low level of the factor " Supportive picture") and the participants' responses on susceptibility to social engineering victimization in Experiments 9, 10, 11, 12, 13, 14, 15, and 16 (as another group since they were given messages that contained a high level of the factor "Supportive picture"). Every group was treated as an experiment, which allowed us to estimate its mean, as presented in Table 6. Assessing every pair of groups was then done using analysis of variance (ANOVA) and Eta-squared effect size.

Partial Eta-squared was used with the ANOVA tests in order to present in the proportion of variance (effect size that ranges from 0–1) in the dependent variable that is explained by the independent variable [108]. While there are no clear-cut rules for evaluating the effect size of this type, Cohen [108] defined effect sizes for Eta-squared as: 0.01 = small effect, 0.06 = moderate effect, 0.14 = large effect. As presented in Table 6, the results of the ANOVA tests demonstrated significant effects of some of the treatments on the susceptibility to social engineering victimization. These treatments include: Spelling (Hypothesis H4) with p value < 0.0001, F value = 614.9 and Eta-squared = 0.169, Grammar (Hypothesis H5) with p value < 0.0001, F value = 317.3 and Eta-squared = 0.174, Message length (Hypothesis H6) with p value < 0.0001, F value = 828.7 and Eta-squared = 0.355, Supportive picture (Hypothesis H7) with p value < 0.0001, F value = 53.865 and Eta-squared = 0.018, Supportive video (Hypothesis H8) with p value < 0.0001, F value = 196.2 and Eta-squared = 0.061, Number of likes (Hypothesis H9) with p value < 0.0001, F value = 4342.5 and Eta-squared = 0.743, and Well-organization (Hypothesis H12) with p value < 0.0001, F value = 443.1 and Eta-squared = 0.227. However, the results of the ANOVA tests showed insignificant effects of Number of comments (Hypothesis H10), with p value = 0.051, F value = 4.677 and Eta-squared = 0.001, and insignificant effects of Emoji (Hypothesis H11), with p value = 0.285, F value = 1.142 and Eta-squared = 0.0003. Based on these results, it was concluded that there was enough evidence to accept hypotheses H4, H5, H6, H7, H8, H9, and H12, and to reject H10 and H11.

Table 6. One-way ANOVA and effect sizes for hypotheses H4–H12.

Constructs	Treatment Group	Cases (N)	Standard Deviation	Mean	F Value	Sig.	Eta Squared	Result
Spelling (Hypothesis: H4)	Low Level	2136	0.36584	2.6159	614.934	<0.0001	0.169	Supported
	High Level	2136	0.46664	2.9946				
Grammar (Hypothesis: H5)	Low Level	2136	0.43868	2.5228	317.325	<0.0001	0.174	Supported
	High Level	2136	0.75236	3.0878				
Message length (Hypothesis: H6)	Low Level	2136	0.34177	2.4019	828.797	<0.0001	0.355	Supported
	High Level	2136	0.68958	3.2088				
Supportive picture (Hypothesis: H7)	Low Level	2136	0.39824	2.7443	53.865	<0.0001	0.018	Supported
	High Level	2136	0.50725	2.8662				
Supportive video (Hypothesis: H8)	Low Level	2136	0.42963	2.6915	196.296	<0.0001	0.061	Supported
	High Level	2136	0.46137	2.9190				
Number of likes (Hypothesis: H9)	Low Level	2136	0.32367	2.2493	4342.588	<0.0001	0.743	Supported
	High Level	2136	0.34938	3.3923				
Number of comments (Hypothesis: H10)	Low Level	2136	0.53982	2.7871	4.677	0.051	0.001	Not Supported
	High Level	2136	0.36231	2.8233				
Emoji (Hypothesis: H11)	Low Level	2136	0.38874	2.7963	1.142	0.285	0.0003	Not Supported
	High Level	2136	0.52158	2.8142				
Well-organization (Hypothesis: H12)	Low Level	2136	0.45186	2.1069	443.154	<0.0001	0.227	Supported
	High Level	2136	0.36344	2.5515				

5.3. Demographics Analysis

ELM suggests that there are individual differences regarding the need for cognition [19]. Therefore, although we have examined the impact of the message's characteristics on the participants' susceptibility to social engineering victimization 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 message's characteristics (which are the treatments given to the participants) and the participants' demographic groups. Table 7 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).

Table 7. Significant interactions between treatment effects and user demographics.

Interaction Specifications					**Effect of the Treatment (Mean Difference) for These Demographic Group**				
Interaction	**F**	**Sig**	**Observed Power**	**P. Eta Square**					
Number of likes with User's Gender	151.7	<0.0001	0.9	0.041	Female			Male	
					2.811			0.94	
Well-organization with User's Educational Level	3.75	<0.0001	0.77	0.005	Lower than Bachelor	Bachelor		Masters	PhD or Doctorate
					0.87	1.25		1.82	2.05
Grammar with User's Educational Level	2.98	0.002	0.74	0.002	Lower than Bachelor	Bachelor		Masters	PhD or Doctorate
					0.99	1.17		1.51	1.75
Number of likes with User's Security Knowledge	6.15	<0.0001	0.98	0.018	Lowest Level	Level 2		Level 3	Highest Level
					0.39	1.11		1.52	1.74
Message length with User's Age	2.54	0.031	0.64	0.008	18–25 Years	26–35	36–45	46-55	56 and Over
					1.07	1.04	1.39	1.58	1.81
Supporting picture with User's Age	3.45	<0.0001	0.86	0.01	18–25 Years	26–35	36–45	46–55	56 and Over
					2.5	1.97	1.92	1.53	1.38
Supportive video with User's Age	2.8	<0.0001	0.71	0.008	18–25 Years	26–35	36–45	46–55	56 and Over
					2.1	1.81	1.92	1.49	1.27
Number of likes with User's Age	3.53	0.001	0.86	0.01	18–25 Years	26–35	36–45	46–55	56 and Over
					3.1	2.21	1.91	1.59	1.22
Message length with User's Educational Level	3.56	0.003	0.81	0.009	Lower than Bachelor	Bachelor		Masters	PhD or Doctorate
					2.71	3.11		3.37	3.76

Although some hypothesized message characteristics were found to induce a significant influence on the users' judgments and decisions for all demographic groups, the results presented in Table 7 show that some message characteristics have even more impact on particular demographic groups. For example, we can see that the number of likes of a message has a statistically significant interaction with the user's gender (F = 151.7, $p < 0.0001$). By running pairwise comparisons, we can see that the number of likes has more impact on females, with a mean difference = 2.811, compared to a mean difference = 0.94 for males. Similarly, we can see that there was a statistically significant interaction between well-organization and a user's educational level, between grammar and user's educational level, between number of likes and user's security knowledge, between message length and user's age, between supporting picture and user's age, between supportive video and user's age, between number of likes and user's age, and between message length and user's educational level. 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 [108]. 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 messages' type of influence. As presented in Table 8, a regression analysis shows that the participants' security knowledge significantly and linearly predicts their susceptibility to social engineering victimization (beta value = −0.18, $p < 0.0001$). 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, 4268) = 241.27, $p < 0.0001$). The results also show that gender has a significant effect on susceptibility to social engineering (beta value = −0.04, $p < 0.001$), with a *t*-test showing that women are more susceptible than men (*t* (4270) = 17.03, $p < 0.0001$). In addition, the results show that the time elapsed since joining Facebook is a significant predictor of susceptibility to social engineering (beta value = −0.12, $p < 0.0001$), and an ANOVA test shows that the less time elapsed, the more susceptible the user is (F(4, 4268) = 10.59, $p < 0.0001$).

Table 8. Regression analysis for demographic groups and group differences.

Regression Analysis			Variance Tests		Means				
Demographic	Standardized Coefficient	Sig	T or F Values	Sig					
Security knowledge	−0.18	<0.0001	F = 241.27	<0.0001	Lowest Level	Level 2		Level 3	Highest Level
					3.09	2.91		2.77	2.73
Gender	−0.04	0.001	T = 17.03	<0.0001	Female			Male	
					2.57			2.41	
Time elapsed since joining Facebook	−0.12	<0.0001	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
					2.91	2.73	2.61	2.64	2.51

Finally, we examined whether any social engineering requests (tricks that were presented in Table 1) have a significantly different impact on any particular demographic group. The rationale behind conducting this analysis is to examine whether any demographic group is more susceptible to a particular trick. For this purpose, we ran a two-way ANOVA to examine the interaction between every particular social engineering request (trick) and every demographic group. The results showed that the participants were affected by the type of social engineering request with no significant difference.

5.4. Testing Mediation Effects

As mentioned in Section 2.2, there is reason to believe that there are some interaction effects between peripheral cues and users' perception of argument quality dimensions and risk. While the analysis showed no moderation effects between peripheral cues and users' perception towards argument quality dimensions and risk, the application of mediation tests in the present study showed some mediations, which we will explain in this section.

A mediator variable is a variable that intervenes in the relationship between independent and dependent variables [109]. To test the mediation using the path coefficient, a variable was added for every message characteristic, thus representing the treatment given to the participants. The additional variables were assigned the number 2 (coded 2) for high levels of each of the message characteristics (treatments), and assigned the number 1 for low levels of each of the message characteristics.

After adding the variables that represented the message characteristics, the mediation effects were examined. Baron et al. [110] have classified mediation as full mediation, partial mediation, or no mediation. Full mediation occurs when the total effect (the path coefficient between the independent and dependent variables without mediation) is statistically significant, while the direct effect (the path coefficient between the independent and dependent variables with mediation) is not significant. Partial mediation occurs when both the total effect and direct effect are significant but the value of the direct effect has been reduced due to the impact of the mediator. No mediation occurs when the total effect is not significant. Other researchers (e.g., References [111–113]) identified an additional type of mediation, namely, suppression mediation, which increases the predictive validity of another variable by its inclusion in a regression equation.

As presented in Table 9, the application of mediation tests in the present study showed that perceived persuasiveness had a partial mediation effect between susceptibility to social engineering victimization and spelling, grammar, supportive picture, supportive video, and well-organization. The application of mediation tests in the present study showed also that perceived informativeness had a partial mediation effect between susceptibility to social engineering victimization and message length and well-organization. Finally, the application of mediation tests in the present study showed that perceived risk had a suppression mediation effect between susceptibility to social engineering victimization and number of likes.

Table 9. Mediation effects.

Relationship			Direct Effect (with mediation)		Type of Mediation
IV	Mediated by	DV	Estimate	*p*	
Spelling	Perceived persuasiveness	Susceptibility to SE	0.09	<0.0001	Partial Mediation
Grammar	Perceived persuasiveness	Susceptibility to SE	0.08	0.008	Partial Mediation
Message length	Perceived informativeness	Susceptibility to SE	0.20	<0.0001	Partial Mediation
Supportive picture	Perceived persuasiveness	Susceptibility to SE	0.13	<0.0001	Partial Mediation
Supportive video	Perceived persuasiveness	Susceptibility to SE	0.16	<0.0001	Partial Mediation
Number of likes	Perceived risk	Susceptibility to SE	0.21	<0.0001	Suppression Mediation
Well-organization	Perceived persuasiveness	Susceptibility to SE	0.12	0.001	Partial Mediation
Well-organization	Perceived informativeness	Susceptibility to SE	0.12	0.003	Partial Mediation

5.5. *Structural Model and Fitting Assessment*

SEM contains several steps including model specification, estimation of free parameters, assessment of model and model fit, and model modification. During "model modification" the model may need to be modified in order to improve the fit, thereby estimating the most likely relationships between variables. As Anderson and Gerbing [114] explain, "Substantive use of structural equation modeling has been growing in psychology and the social sciences. One reason for this is that these confirmatory methods provide researchers with a comprehensive means for assessing and modifying theoretical models". In this study, model fit assessment was performed using AMOS (version 22.0), which provides modification indices that guide some modifications (e.g., adding mediations' relationships). We found that adding mediation effects (relationships) to the model has improved the model fit, therefore making these changes to the hypothesized theory (a priori model), which is claimed to be true.

One of the objectives of performing model fit assessment is to confirm whether the collected data are an appropriate fit for the hypothesized model. The values of the correlations between perceived informativeness, perceived persuasiveness, perceived risk, and susceptibility to social engineering victimization provided an indication of the discriminant validity, where all correlations were less than 0.55 between the independent constructs and less than 0.70 when both independent and dependent constructs were included. This validity refers to the extent to which a construct is distinct from other constructs [115]. In addition, all the factor loadings were high and significant at the $p < 0.01$ level, suggesting convergent validity. This validity refers to the degree to which an item is related to the construct [115]. We can see in Figure 1 that some values (e.g., beta values and model fit) are not identical to the results of SPSS, which were presented in Table 5. This difference occurred due to the application of mediation tests, which reduced the beta values of the direct effects in the case of partial mediations, increased it in the case of suppression mediations, and improved the overall model fit (from $R^2 = 0.46$–$R^2 = 0.49$).

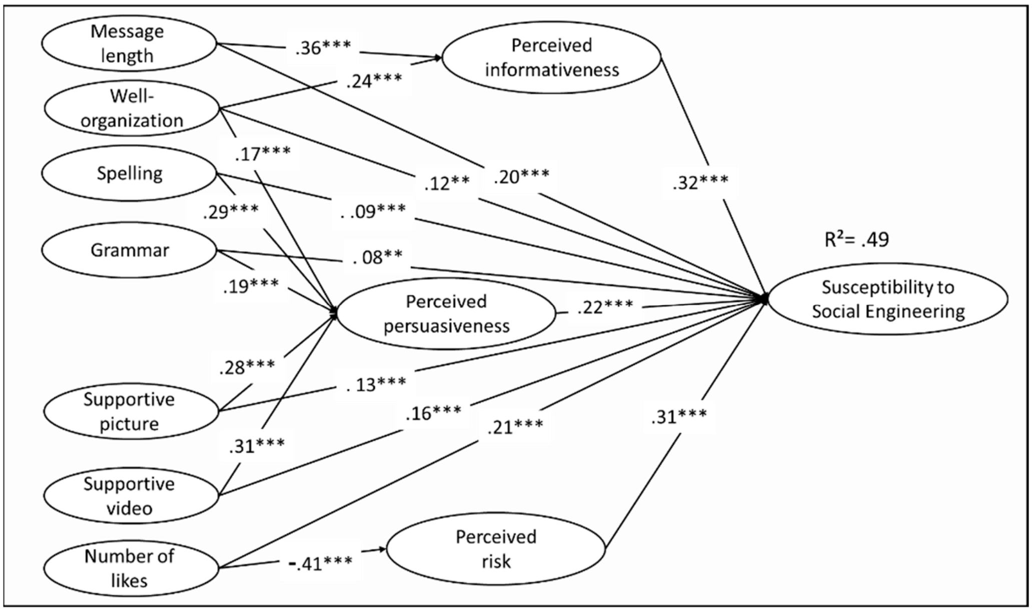


Figure 1. The research model.

In addition, assessments were done in regard to the goodness of fit. The resultant model appears to have a good fit, with the following values: Minimum discrepancy (chi-square, χ^2) divided by the degrees of freedom (df) = 3.45; goodness of fit index (GFI) = 0.91; comparative fit index (CFI) = 0.97; incremental fit index (IFI) = 0.96; and root mean square error of approximation (RMSEA) = 0.021. These values satisfy the requirements suggested by structural equation modeling [115,116].

6. Discussion and Conclusion

6.1. Implication for Research and Practice

Social engineering in SNSs is a major issue in information security; however, other than anecdotal materials, there is little to help managers, organizations, and researchers to address the problem because the relationships among personal judgment, perception, and social engineering outcomes have not been thoroughly investigated. By realizing the strong impact of message characteristics on users' susceptibility to social engineering victimization, this study showed what, and to what extent, factors make social engineering tricks successful on Facebook. This has been done through investigating the effects of the central route of persuasion, peripheral route of persuasion, and perceived risk on susceptibility to social engineering victimization.

The contribution of this study appears to be unique and useful in relation to the prediction and detection of users' susceptibility. The study identified 7 message characteristics that play a vital role in influencing users to accept social engineering attacks. By considering the question of how the vulnerabilities of a given user can be predicted, the results of this study have shown that susceptibility to social engineering victimization can be predicted by every factor of perceived informativeness of a message, perceived persuasiveness of a message, perceived risk of a message, spelling of a message, grammar of a message, message length, having supportive picture in a message, having supportive video in a message, number of likes of a message, and organization of a message. All the hypothesized paths were found significant except hypothesis 10 and hypothesis 11. The resultant model showed an adequate percentage of the variance explained, with the overall model fit of $R^2 = 0.49$. Perceived informativeness was found to induce the most influence on users' judgment toward accepting or rejecting social engineering-based attacks on Facebook, then perceived risk, then perceived persuasiveness, and then the peripheral cues that have been explored in this study.

Furthermore, by realizing that human susceptibility to social engineering threats will be different from context-to-context and from person-to-person, and by realizing that users' perceptions of threat and risk are affected by many factors such as risk belief, awareness level, and users' demographics, this study investigated the relationship between the effect of central route of persuasion, peripheral route of persuasion, perceived risk and demographic variables. The results of the demographics analysis showed that some demographic groups are more susceptible to social engineering victimization in general (those with lower security knowledge, females, those with less time elapsed since joining Facebook). In addition, some of the message characteristics were found to induce even more impact on particular demographic groups. That is, there was a statistically significant interaction between the number of likes of a message and the user's gender, between well-organization and the user's educational level, between grammar and the user's educational level, between number of likes and the user's security knowledge, between message length and the user's age, between supporting picture and the user's age, between supportive video and the user's age, between number of likes and the user's age, and between message length and the user's educational level. The results of this study also showed some important mediation effects between central route, perceived risk, peripheral cues, and susceptibility to social engineering.

The results of the demographics analysis are important in many ways. First, it has been found that security knowledge significantly and linearly predicts users' susceptibility to social engineering victimization. This result provides more validity in regard to the questions and the method 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 result showed that the participants were affected by the type of social engineering request with no significant difference. This result provides an indication that the majority of the participants in this study relied on the treatments used in the experiments, and therefore, it provides more validity regarding the resulted model. Third, the results have shown that demographic groups differ in their perceptions and behaviors toward social engineering requests. This difference is significantly affected by the message characteristics used in a social engineering trick. Therefore, measuring susceptibility to social engineering should be done by using the type of persuasion, and not only whether the user became a victim or not, as has been done repeatedly in phishing e-mail studies (e.g., References [6,12,32–36]). The resulted mediation effects provide a deep explanation of ELM. That is, ELM suggests that there are two types of factors, which influence how and how much the recipient can elaborate on a message. The first type is the factors that influence the recipient's motivation to elaborate, and the second type is the factors that influence the recipient's ability to elaborate [18]. The resulted mediation effects of the present study explained this process through explaining how some of the explored peripheral cues, such as message organization, having supporting picture, having supporting video, can influence the recipients to be motivated, or if they are able to elaborate, and therefore affect the process to be shifted from peripheral route to central route of persuasion. The resulted model also explains the different ways of processing stimuli, and their outcomes on users' cognition and intention to accept (fall victim to) social engineering tricks. To the best of the author's knowledge, this study was the first study to be dedicated to explaining this process in terms of social engineering in SNSs, or even in real life situations.

Furthermore, to the best of the author's knowledge, this study was the first study to be dedicated to understanding which demographic factors correlate with the influence of different message characteristics toward social engineering victimization on SNSs. Therefore, in order to compare the results of this research with those reported previously, we will use the closest studies that this study can be compared with. The results of this study showed that the participants' security knowledge significantly and linearly predicted their susceptibility to social engineering victimization. The results of an ANOVA comparing the security knowledge groups showed that, the more security knowledge the participants had, the less susceptible they were. This result is similar to the findings of Algarni et al. [23] who reported a similar relationship. This result is also similar to the findings in the literature that participants who had undertaken anti-phishing training were less susceptible to victimization [117]. Although anti-phishing training does not necessarily infer security knowledge, it is the closest demographic factor that the present study's results can be compared with.

The results of this study showed that gender had a significant effect on susceptibility to social engineering victimization, with females being more susceptible than male users. This result is similar to the findings in the literature that females were more susceptible to email phishing victimization [35,117] and were more susceptible to social engineering victimization on Facebook (Algarni et al. [23]). Moreover, the results of this study showed that the less time elapsed since joining Facebook, the more susceptible the user. This is in line also with the findings reported by Algarni et al. [23]. On the other hand, while some phishing emails studies (e.g., References [35,117]) reported a relationship between susceptibility to phishing victimization and other demographics, such as age and educational level, these demographics have not been found statistically significant in this study. In addition, Vishwanath [118] found that habitual Facebook use (measured by the participant's frequent use of Facebook, maintenance of a large social network, and limited ability to regulate behavior) was a significant predictor of phishing victimization on Facebook. Among the three factors that Vishwanath [118] used to measure habitual Facebook use, the maintenance of a large social network (participants' number of friends) and the frequency of Facebook usage were also examined in the present study. However, neither were found to be significant predictors of social engineering victimization in this study. This neither endorses nor rejects the findings reported previously in the literature, as every study is impacted by its sample size, or other factors outside of the study scope. Moreover, the findings of the present study were drawn from an investigation of five social engineering tricks, while Vishwanath studied the phishing technique only. This may explain the difference between these results.

Some interesting observations arise from the analysis of the interaction between demographic groups and susceptibility to social engineering victimization (please refer to Table 8), or interactions between the effects of the message's characteristics and the participants' demographic groups (please refer to Table 7). While some of these effects and interactions can be interpreted, or partially understood, most of them require further research. For example, the results of this study showed that gender had a significant effect on susceptibility to social engineering victimization, with the t-test results showing that female users were more susceptible than male users. Sheng et al. [35] sought an explanation for why gender affects susceptibility to phishing victimization and suggested that the high level of susceptibility among female users was attributable to female users having less technical experience than male users.

However, providing valid explanations for some interactions fall beyond the scope of this study. For example, the results showed that there is a significant interaction between the number of likes and gender, and significant interaction between the number of likes and age. A closer look into the research that investigated liking on Facebook reveals that the meaning of Likes remains unclear. For example, Hong et al. [119] argues that liking on Facebook can be perceived as a form of online gift giving, Lee et al. [120] suggest that liking on Facebook could be seen as a cue for social affirmation, Burrow and Rainone [121] interpret liking on Facebook as a signal for social acceptance, Scissors et al. [122] argue that Likes are social cues expressing social appropriateness, and Meshi et al. [123] interpret liking on Facebook as a form of positive feedback. Therefore, given the complexity of the meaning of a factor such as Liking and its impact on users, it is important to be careful when interpreting such interactions. A valid explanation can be obtained in most cases through conducting a further and perhaps specific research dedicated to understanding why specific demographics group influenced by specific treatment (e.g., Likes), and this is an opportunity for future research.

The findings of this study have a number of important implications. First, the aims of this research, the methodology used and the findings help to fill an important gap in the information systems literature. Cao et al. [124] concluded a review of SNS research published in major information systems journals between January 2004 and August 2013 with the call for future research to focus on the validation of constructs and development of theories that are specific to SNSs, to investigate the individual characteristics or factors that play a role in SNS research, and to employ multiple research methods including qualitative methods and data analytics.

Second, understanding the cognition, attitudes, behavioral intentions, and behavioral compliance of individuals in response to attacks is a key element in information security. This study makes a practical contribution to addressing the high risk of social engineering in SNSs. This can be seen by comparing the scope of this study with the social engineering solutions proposed in the literature for SNSs such as spamming, bot-operated accounts, and cloning detection. All of the proposed solutions focus on technology. Notwithstanding the importance of those solutions, this study's focus is on the main and weakest link, namely, the user. None of the social engineering-based attacks could succeed unless the users themselves accept, succumb and perform the requested action. The concept of social engineering is relatively new to information technology, poses significant security risks, and is challenging to control [1,125]. By pinpointing some of the key elements in a user's decision to accept or reject social engineering attacks, the findings from the current study represent a crucial step towards understanding user susceptibility to social engineering attacks in SNSs. The setting of the study also reflects the significance of the contribution, as SNSs are now believed to be the most common source of social engineering attacks [10–13,126].

Furthermore, while the contribution of this research is of particular relevance to the knowledge of social engineering in SNSs, the findings of this study make a significant contribution to the knowledge in several other areas. For example, this study tested the existence of two dimensions of argument quality, and proposed the peripheral cues that are related to a message in the environment of Facebook, which have not been reported in all previous studies; thus establishing the study's significant contribution toward the existing knowledge on several areas of study such as deception, persuasion, and human communication. While argument quality has been a topic of much focus in the context of marketing such as evaluating online vendors, buying tangible products online, or evaluation of users' reviews, the findings of this study significantly extend prior research by developing and empirically testing a theory-grounded model of the heuristic-systematic and ELM on social engineering in SNSs.

In addition, the way in which this study investigates the impact of demographic variables on susceptibility to social engineering attacks appears to be unique. Studies conducted on phishing attacks (which also usually use social engineering-based persuasion but in a different environment from SNSs) have indicated that there is a relationship between falling victim to phishing emails and demographic variables such as age, gender, and educational level [117]. However, the present study investigates social engineering victimization in a new environment, (Facebook), and goes further by investigating the relationship between demographic variables and message characteristics used by attackers to persuade users.

One of the important implications of the findings of this study is that identifying the links between the message's characteristics and the users' (as receivers) characteristics is a valuable achievement 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. Profiling users is a practical solution that has been established. Several studies in the literature have successfully established solutions based on Facebook user profiling for the purpose of managing relationships between users (e.g., [127–130]), predicting users' privacy behaviors or threats (e.g., [131,132]), classifying users' relationships (e.g., [133]), and detecting similarity between contents, topics, or writing styles (e.g., [134]). Looking at the identified peripheral cues that have been explored in this study, we can see that they are even more measurable and useful than those variables used in previous profiling mechanisms.

The findings of this study are also very useful for raising awareness among individuals and employees who have been known as the weakest link in the cyber-security chain [135]. Individuals and employees' ability to detect deception is even more limited in a virtual environment such as Facebook. The findings of this study can be used to raise awareness through security education, training, and awareness programs (SETA programs), computer monitoring, and policy-making, all of which have been suggested as best practices for deterring human-based information security incidents [136].

6.2. Limitations and Future Work

The findings of this research must be viewed in light of the following limitations. The first issue is regarding the use of role-play experiment. 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., References [23,34,35,88–90,137–140]). 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. In addition, the validity of the research conducted in this study was enhanced through the use of well-known strategy, commonly used in deception research, which involves hiding (by not telling) the true purpose of the study. The participants were told at the beginning of the experiment that the study aimed to investigate the usability of Facebook in general, and they were told the true purpose after the experiment concluded. This practice has been found to be a very effective strategy, useful, and morally justifiable in experimental research [141,142]. Furthermore, the results of the demographics analysis, as explained in the results section, provided more validity that the experiment mimicked real-life situations. In real life, social engineering tricks are more identifiable by people who are knowledgeable about security than by normal users, including highly educated people in different study areas, and the same phenomenon was observed in this study.

The second issue is regarding the use of social engineering tricks. 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. 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 message characteristics that influence users to fall victim to, and therefore a few social engineering tricks can be sufficient. The third limitation relates to the participants and the sample of the second phase. The participants were chosen from two organizations located in Saudi Arabia and the United Arab Emirates. This means that the sample did not include all demographics, such as all religions or cultures. However, this is common practice in behavior research, as it would be impossible due to geographical isolation, time, and funding limitations to include all demographics.

Finally, there are several recommendations and suggestions regarding future research in this area. First, since this study focused on the impact of message characteristics on users' susceptibility to social engineering victimization, future research could focus on investigating SNS environments and their impact on users' susceptibility to social engineering victimization. Second, since this study focused on Facebook as the context of the research, future research could focus on expanding the findings by utilizing more samples that are representative of various SNSs, and more samples that are representative of various countries and cultures. As every research has its limitations, future researchers can also utilize other creative methodologies to avoid the limitations of this study, such as examining whether the findings from an experiment in the actual Facebook environment are different to the findings from the role-play experiment. Finally, 49% of variances in susceptibility to social engineering victimization are explained in the research model. This suggests that some other important predictors may be missing. Future researchers are highly recommended to investigate what have been found as significant predictors in the context of online reviews, electronic word-of-mouth communication, internet shopping, online purchasing intention, and online information adaption (e.g., References [57,143–145]). The findings of these studies may provide valuable insight into potential factors and relationships underlying susceptibility to social engineering in SNSs.

Funding: This research received no external funding.

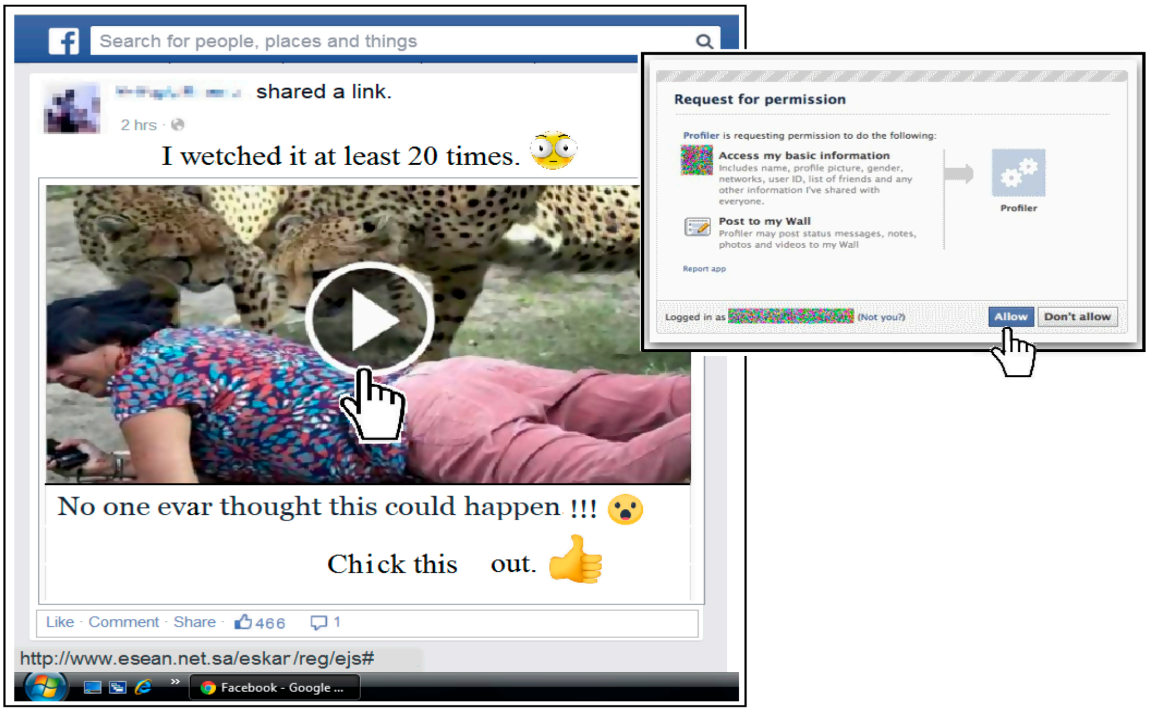
Conflicts of Interest: The author declares no conflict of interest.

Appendix A Appendix

Question: If you come across the following message on Facebook (Figure A1), would you give the permission to the application?

Answer:

□ Definitely yes
□ Very probably yes
□ Probably yes
□ Very probably no
□ Definitely no



Search for people, places and things

[redacted] shared a link.

2 hrs ·

I wetched it at least 20 times.

No one evar thought this could happen !!!

Chick this out.

Like · Comment · Share · 466
1

http://www.esean.net.sa/eskar/reg/ejs#

Request for permission

Profiler is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.

Post to my Wall
Profiler may post status messages, notes, photos and videos to my Wall

Logged in as [redacted] (Not you?)

Figure A1. Experiment's Example.

References

1. Hadnagy, C. *Social Engineering: The Art of Human Hacking*; Wiley: Hoboken, NJ, USA, 2010.
2. Thornburgh, T. Social Engineering: The Dark Art. In Proceedings of the 1st Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 8 October 2004; ACM: New York, NY, USA; pp. 133–135.
3. Workman, M. Gaining Access with Social Engineering: An Empirical Study of the Threat. *Inf. Syst. Secur.* **2007**, *16*, 315–331. [CrossRef]
4. Grazioli, S. Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet. In *Group Decision and Negotiation*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 13, pp. 149–172.
5. Qi, T. An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. In Proceedings of the 2007 IEEE Intelligence and Security Informatics, New Brunswick, NJ, USA, 23–24 May 2007; pp. 152–159.
6. Kvedar, D.; Nettis, M.; Fulton, S.P. The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *J. Comput. Sci. Coll.* **2010**, *26*, 80–87.
7. Algarni, A.; Xu, Y.; Chan, T.; Tian, Y.-C. Social Engineering in Social Networking Sites: Affect-Based Model. In Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 9–12 December 2013; pp. 508–515.
8. Algarni, A.; Xu, Y.; Chan, T.; Tian, Y.-C. Toward Understanding Social Engineering. In *Law & Practice: Critical Analysis and Legal Reasoning*; Sylvia, K., Ed.; International Association of IT Lawyers: Copenhagen, Denmark, 2013; pp. 279–300.
9. Braun, R.; Esswein, W. Towards a Conceptualization of Corporate Risks in Online Social Networks: A Literature Based Overview of Risks. In Proceedings of the 17th IEEE International Enterprise Distributed Object Computing Conference (EDOC), Vancouver, BC, Canada, 9–13 September 2013; pp. 267–274.
10. Chitrey, A.; Singh, D.; Singh, V. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. *Int. J. Inf. Netw. Secur.* **2012**, *1*, 45–53. [CrossRef]
11. Dimensional-Research. *The Risk of Social Engineering on Information Security: A Survey of It Professionals*; Technical Report; Dimensional-Research: Long Beach, CA, USA, 2011.

12. Jagatic, T.N.; Johnson, N.A.; Jakobsson, M.; Menczer, F. Social phishing. *Commun. ACM* **2007**, *50*, 94–100. [CrossRef]
13. Nagy, J.; Pecho, P. Social Networks Security. In Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies, Athens/Glyfada, Greece, 18–23 June 2009; pp. 321–325.
14. Mazzuca, T. *7 Scary Findings from the 2014 Symantec Internet Security Threat Report*; Property & Casualty 360; Red Rock Casino Resort & Spa: Las Vegas, NV, USA, 2014.
15. Chaiken, S.; Eagly, A.H. *Heuristic and Systematic Information Processing within and Beyond the Persuasion Context*; In Unintended Thought; Wiley: Hoboken, NJ, USA, 1989; pp. 212–252.
16. Chen, S.; Chaiken, S. The Heuristic-Systematic Model in Its Broader Context. In *Dual-Process Theories in Social Psychology*; Guilford Press: New York, NY, USA, 1999; pp. 73–96.
17. Darke, P.R.; Freedman, J.L.; Chaiken, S. Percentage discounts, initial price, and bargain hunting: A heuristic-systematic approach to price search behavior. *J. Appl. Psychol.* **1995**, *80*, 580–586. [CrossRef]
18. Petty, R.E.; Cacioppo, J. Elaboration Likelihood Model. In *Handbook of Theories of Social Psychology*; Sage: London, UK, 1986.
19. Petty, R.E.; Cacioppo, J.T. The elaboration likelihood model of persuasion. *Adv. Exp. Soc. Psychol.* **1986**, *19*, 123–205.
20. Petty, R.E.; Cacioppo, J.T. The Elaboration Likelihood Model of Persuasion. In *Communication and Persuasion*; Springer: Berlin/Heidelberg, Germany, 1986; pp. 1–24.
21. Algarni, A.; Xu, Y.; Chan, T. Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook. In Proceedings of the 36th International Conference on Information Systems (ICIS 2015), Fort Worth, TX, USA, 13–16 December 2015.
22. Algarni, A.; Xu, Y.; Chan, T. Measuring Source Credibility of Social Engineering Attackers on Facebook. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 3686–3695.
23. Algarni, A.; Xu, Y.; Chan, T. An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *Eur. J. Inf. Syst.* **2017**, 1–27. [CrossRef]
24. Gu, J.; Xu, Y.C.; Xu, H.; Zhang, C.; Ling, H. Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decis. Support Syst.* **2017**, *94*, 19–28. [CrossRef]
25. Li, C.-Y. The effects of source credibility and argument quality on employees' responses toward information system usage. *Asia Pac. Manag. Rev.* **2015**, *20*, 56–64. [CrossRef]
26. Mun, Y.Y.; Yoon, J.J.; Davis, J.M.; Lee, T. Untangling the antecedents of initial trust in Web-based health information: The roles of argument quality, source expertise, and user perceptions of information quality and risk. *Decis. Support Syst.* **2013**, *55*, 284–295.
27. Petty, R.E.; Cacioppo, J.T. Issue involvement can increase or decrease persuasion by enhancing message-relevant cognitive responses. *J. Personal. Soc. Psychol.* **1979**, *37*, 1915–1926. [CrossRef]
28. Petty, R.E.; Cacioppo, J.T. The effects of involvement on responses to argument quantity and quality: Central and peripheral routes to persuasion. *J. Personal. Soc. Psychol.* **1984**, *46*, 69–81. [CrossRef]
29. Petty, R.E.; Cacioppo, J.T.; Schumann, D. Central and peripheral routes to advertising effectiveness: The moderating role of involvement. *J. Consum. Res.* **1983**, *10*, 135–146. [CrossRef]
30. Shin, S.Y.; Van Der Heide, B.; Beyea, D.; Dai, Y.N.; Prchal, B. Investigating moderating roles of goals, reviewer similarity, and self-disclosure on the effect of argument quality of online consumer reviews on attitude formation. *Comput. Hum. Behav.* **2017**, *76*, 218–226. [CrossRef]
31. Maconachy, W.V.; Schou, C.D.; Ragsdale, D.; Welch, D. A Model for Information Assurance: An Integrated Approach. In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, West Point, NY, USA, 5–6 June 2001.
32. Kumaraguru, P.; Cranshaw, J.; Acquisti, A.; Cranor, L.F.; Hong, J.; Blair, M.A.; Pham, T. *School of Phish: A Real-Word Evaluation of Anti-Phishing Training (Cmu-Cylab-09-002)*; Carnegie Mellon University: Pittsburgh, PA, USA, 2009.
33. Parrish, J.L., Jr.; Bailey, J.L.; Courtney, J.F. *A Personality Based Model for Determining Susceptibility to Phishing Attacks*; University of Arkansas: Little Rock, AR, USA, 2009.
34. Pattinson, M.; Jerram, C.; Parsons, K.; McCormac, A.; Butavicius, M. Why do some people manage phishing e-mails better than others? *Inf. Manag. Comput. Secur.* **2012**, *20*, 18–28. [CrossRef]

35. Sheng, S.; Holbrook, M.; Kumaraguru, P.; Cranor, L.F.; Downs, J. 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, NY, USA, 10–15 April 2010; pp. 373–382.
36. Workman, M. Wisecrackers: A theory–grounded investigation of phishing and pretext social engineering threats to information security. *J. Am. Soc. Inf. Sci. Technol.* **2008**, *59*, 662–674. [CrossRef]
37. Wright, R.T.; Jensen, M.L.; Thatcher, J.B.; Dinger, M.; Marett, K. Research Note-Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Inf. Syst. Res.* **2014**, *25*, 385–400. [CrossRef]
38. Algarni, A. Inattentional Blindness Factors that Make People Vulnerable to Security Threats in Social Networking Sites. *J. Comput.* **2019**, *14*, 184–194.
39. Castillo, C.; Mendoza, M.; Poblete, B. Information Credibility on Twitter. In Proceedings of the 20th International Conference on the World Wide Web, Hyderabad, India, 28 March–1 April 2011; ACM: New York, NY, USA, 2011; pp. 675–684.
40. Chu, Z.; Gianvecchio, S.; Wang, H.; Jajodia, S. Detecting automation of twitter accounts: Are you a human, bot, or cyborg? *IEEE Trans. Depend. Secur. Comput.* **2012**, *9*, 811–824. [CrossRef]
41. Huber, M.; Kowalski, S.; Nohlberg, M.; Tjoa, S. Towards Automating Social Engineering Using Social Networking Sites. In Proceedings of the CSE'09 International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 29–31 August 2009; pp. 117–124.
42. McCord, M.; Chuah, M. Spam Detection on Twitter Using Traditional Classifiers. In *Autonomic and Trusted Computing*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 175–186.
43. Stringhini, G.; Kruegel, C.; Vigna, G. Detecting Spammers on Social Networks. In Proceedings of the 26th Annual Computer Security Applications Conference, Austin, TX, USA, 6–10 December 2010; pp. 1–9.
44. Thomas, K.; McCoy, D.; Grier, C.; Kolcz, A.; Paxson, V. 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, 14–16 August 2013; pp. 195–210.
45. Wang, A.H. Don't Follow Me: Spam Detection in Twitter. In Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT), Athens, Greece, 26–28 July 2010; pp. 1–10.
46. Algarni, A.; AlMakrami, H.; Alarifi, A. Toward Evaluating Trustworthiness of Social Networking Site Users: Reputation-Based Method. *Arch. Bus. Res.* **2019**, *7*. [CrossRef]
47. Al Zamal, F.; Liu, W.; Ruths, D. 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, 4–8 June 2012; Association for the Advancement of Artificial Intelligence: Menlo Park, CA, USA, 2012; pp. 387–390.
48. Burger, J.D.; Henderson, J.; Kim, G.; Zarrella, G. Discriminating Gender on Twitter. In Proceedings of the Conference on Empirical Methods in Natural Language Processing, Edinburgh, UK, 27–31 July 2011; pp. 1301–1309.
49. Liu, W.; Ruths, D. *What's in a Name? Using First Names as Features for Gender Inference in Twitter*; AAAI Spring Symposium: Analyzing Microtext; AAAI: Menlo Park, CA, USA, 2013.
50. Mislove, A.; Lehmann, S.; Ahn, Y.-Y.; Onnela, J.-P.; Rosenquist, J.N. Understanding the Demographics of Twitter Users. In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Barcelona, Spain, 17–21 July 2011; Association for the Advancement of Artificial Intelligence: Menlo Park, CA, USA, 2011; pp. 1–4.
51. Rao, D.; Paul, M.J.; Fink, C.; Yarowsky, D.; Oates, T.; Coppersmith, G. Hierarchical Bayesian Models for Latent Attribute Detection in Social Media. In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Barcelona, Spain, 17–21 July 2011; pp. 598–601.
52. Cheung, C.M.; Chiu, P.Y.; Lee, M.K. Online social networks: Why do students use Facebook? *Comput. Hum. Behav.* **2011**, *27*, 1337–1343. [CrossRef]
53. Papacharissi, Z. The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn and ASmallWorld. *New Med. Soc.* **2009**, *11*, 199–220. [CrossRef]
54. Trumbo, C.W. Heuristic-systematic information processing and risk judgment. *Risk Anal.* **1999**, *19*, 391–400. [CrossRef] [PubMed]
55. Trumbo, C.W. Information processing and risk perception: An adaptation of the Heuristic-Systematic model. *J. Commun.* **2002**, *52*, 367–382. [CrossRef]

56. Lee, J.K.; Rao, H.R. Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment. *Decis. Support Syst.* **2007**, *43*, 1431–1449. [CrossRef]
57. Cheung, C.M.; Thadani, D.R. The impact of electronic word-of-mouth communication: A literature analysis and integrative model. *Decis. Support Syst.* **2012**, *54*, 461–470. [CrossRef]
58. Li, M.; Kankanhalli, A.; Kim, S.H. Which ideas are more likely to be implemented in online user innovation communities? An empirical analysis. *Decis. Support Syst.* **2016**, *84*, 28–40. [CrossRef]
59. Cheung, M.Y.; Luo, C.; Sia, C.L.; Chen, H. Credibility of electronic word-of-mouth: Informational and normative determinants of on-line consumer recommendations. *Int. J. Electron. Commer.* **2009**, *13*, 9–38. [CrossRef]
60. Zhang, K.Z.; Zhao, S.J.; Cheung, C.M.; Lee, M.K. Examining the influence of online reviews on consumers' decision-making: A heuristic–systematic model. *Decis. Support Syst.* **2014**, *67*, 78–89. [CrossRef]
61. Zhang, Y. Responses to humorous advertising: The moderating effect of need for cognition. *J. Advert.* **1996**, *25*, 15–32. [CrossRef]
62. Burke, K. *Language as Symbolic Action: Essays on Life, Literature, and Method*; University of California Press: Oakland, CA, USA, 1966.
63. Cheung, C.M.; Lee, M.K.; Rabjohn, N. The impact of electronic word-of-mouth: The adoption of online opinions in online customer communities. *Internet Res.* **2008**, *18*, 229–247. [CrossRef]
64. Lee, J.; Lee, J.-N. Understanding the product information inference process in electronic word-of-mouth: An objectivity–subjectivity dichotomy perspective. *Inf. Manag.* **2009**, *46*, 302–311. [CrossRef]
65. Sussman, S.W.; Siegal, W.S. Informational influence in organizations: An integrated approach to knowledge adoption. *Inf. Syst. Res.* **2003**, *14*, 47–65. [CrossRef]
66. Zhang, W.; Watts, S.A. Capitalizing on content: Information adoption in two online communities. *J. Assoc. Inf. Syst.* **2008**, *9*, 3.
67. Ducoffe, R.H. Advertising value and advertising on the web. *J. Advert. Res.* **1996**, *36*, 21.
68. Rosenstock, I.M. Historical origins of the health belief model. *Health Educ. Behav.* **1974**, *2*, 328–335. [CrossRef]
69. Posey, C.; Roberts, T.L.; Lowry, P.B.; Hightower, R.T. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Inf. Manag.* **2014**, *51*, 551–567. [CrossRef]
70. Aldoory, L.; Van Dyke, M.A. The roles of perceived "shared" involvement and information overload in understanding how audiences make meaning of news about bioterrorism. *J. Mass Commun. Q.* **2006**, *83*, 346–361. [CrossRef]
71. Grunig, J.E.; Moss, D.; MacMANUS, T. *A Situational Theory of Publics: Conceptual History, Recent Challenges and New Research*; In Public Relations Research: An International Perspective; International Thomson Business Press: Stamford, CT, USA, 1997; p. 48.
72. Brafman, O.; Brafman, R. *Click: The Forces Behind How We Fully Engage with People, Work, and Everything We Do*; Crown Pub.: New York, NY, USA, 2011.
73. Zimbardo, P. *The Lucifer Effect: Understanding How Good People Turn Evil*; Blackwell Publishing Ltd.: New York, NY, USA, 2007.
74. Orgill, G.L.; Romney, G.W.; Bailey, M.G.; Orgill, P.M. The Urgency for Effective User Privacy-Education to Counter Social Engineering Attacks on Secure Computer Systems. In Proceedings of the 5th Conference on Information Technology Education, Salt Lake City, UT, USA, 28–30 October 2004; pp. 177–181.
75. Pyszczynski, T.; Greenberg, J.; Solomon, S. Why Do We Need What We Need? A Terror Management Perspective on the Roots of Human Social Motivation. *Psychol. Inq.* **1997**, *8*, 1–20. [CrossRef]
76. Cheung, C.M.; Lee, M.K. Trust in internet shopping: Instrumental development and validation through classical and modern approaches. *Adv. Top. Glob. Inf. Manag.* **2001**, *1*, 25–41. [CrossRef]
77. Taking, R. *Information Handling in Consumer Behaviour*; Cox, D.F., Ed.; Boston Graduate School of Business Administration, Harvard University: Boston, MA, USA, 1967.
78. Nicolaou, A.I.; McKnight, D.H. Perceived information quality in data exchanges: Effects on risk, trust, and intention to use. *Inf. Syst. Res.* **2006**, *17*, 332–351. [CrossRef]
79. Cheung, C.M.; Chan, G.W.; Limayem, M. A critical review of online consumer behavior: Empirical research. *J. Electron. Commer. Org.* **2005**, *3*, 1–19. [CrossRef]

80. Metzger, M.J.; Flanagin, A.J.; Eyal, K.; Lemus, D.R.; McCann, R.M. Credibility for the 21st century: Integrating perspectives on source, message, and media credibility in the contemporary media environment. *Commun. Yearb.* **2003**, *27*, 293–336. [CrossRef]
81. Kane, G.C.; Alavi, M.; Labianca, G.J.; Borgatti, S.P. What's Different About Social Media Networks? A Framework and Research Agenda. *Mis Q.* **2014**, *38*, 274–304. [CrossRef]
82. Creswell, J.W. *Qualitative Inquiry and Research Design: Choosing among Five Approaches*; Sage Publications: Thousand Oaks, CA, USA, 2012.
83. Sutton, S.G.; Arnold, V. Focus group methods: Using interactive and nominal groups to explore emerging technology-driven phenomena in accounting and information systems. *Int. J. Account. Inf. Syst.* **2013**, *14*, 81–88. [CrossRef]
84. Hausman, A.V.; Siekpe, J.S. The effect of web interface features on consumer online purchase intentions. *J. Bus. Res.* **2009**, *62*, 5–13. [CrossRef]
85. Metzger, M.J.; Flanagin, A.J. Credibility and trust of information in online environments: The use of cognitive heuristics. *J. Pragmat.* **2013**, *59*, 210–220. [CrossRef]
86. Castillo, C.; Mendoza, M.; Poblete, B. Predicting information credibility in time-sensitive social media. *Internet Res.* **2013**, *23*, 560–588. [CrossRef]
87. Yardley-Matwiejczuk, K.M. *Role Play: Theory and Practice*; Sage Publications: London, UK, 1997.
88. Dhamija, R.; Tygar, J.D.; Hearst, M. Why Phishing Works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montréal, QC, Canada, 22–27 April 2006; pp. 581–590.
89. Downs, J.S.; Holbrook, M.; Cranor, L.F. Behavioral Response to Phishing Risk. In Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, Pittsburgh, PA, USA, 4–5 October 2007; pp. 37–44.
90. Furnell, S. Phishing: Can We Spot the Signs? *Comput. Fraud Secur.* **2007**, *2007*, 10–15. [CrossRef]
91. Baltazar, J.; Costoya, J.; Flores, R. The real face of koobface: The largest web 2.0 botnet explained. *Trend Micro Res.* **2009**, *5*, 10.
92. Baumhof, V.; Shipp, A. *Zeus P2p Advancements and Mitb Attack Vectors*; ThreatMetrix™ Labs Public Report; ThreatMetrix Inc.: San Jose, CA, USA, 2012; 2p.
93. Clark, K. Five Notorious Facebook Attacks (Learn How to Protect Yourself). *Soc. Med.* **2013**. Available online: http://www.hongkiat.com/blog/five-facebook-attacks/ (accessed on 2 March 2015).
94. Sadeghian, A.; Zamani, M.; Shanmugam, B. Security Threats in Online Social Networks. In Proceedings of the 2013 International Conference on Informatics and Creative Multimedia (ICICM), Kuala Lumpur, Malaysia, 4–6 September 2013; pp. 254–258.
95. Thomas, K.; Nicol, D.M. 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, 19–20 October 2010; pp. 63–70.
96. Albaum, G. The Likert Scale Revisited, *J. Mark. Res. Soc.* **1997**, *39*, 331–348. [CrossRef]
97. Gunst, R.F.; Mason, R.L. Fractional factorial design. *Wiley Interdiscip. Rev. Comput. Stat.* **2009**, *1*, 234–244. [CrossRef]
98. Dey, A. *Orthogonal Fractional Factorial Designs*; Wiley: New York, NY, USA, 1985.
99. DeVellis, R.F. *Scale Development: Theory and Applications*; Sage Publications: Thousand Oaks, CA, USA, 2012.
100. Ducoffe, R.H. How consumers assess the value of advertising. *J. Curr. Issues Res. Advert.* **1995**, *17*, 1–18. [CrossRef]
101. Dowling, G.R.; Staelin, R. A model of perceived risk and intended risk-handling activity. *J. Consum. Res.* **1994**, *21*, 119–134. [CrossRef]
102. Coates, J.F. In defense of Delphi. A review of Delphi assessment, expert opinion, forecasting, and group process by H. Sackman. *Technol. Forecast. Soc. Chang.* **1975**, *7*, 193–194. [CrossRef]
103. Dalkey, N.; Helmer, O. An experimental application of the Delphi method to the use of experts. *Manag. Sci.* **1963**, *9*, 458–467. [CrossRef]
104. Sivo, S.A.; Saunders, C.; Chang, Q.; Jiang, J.J. How low should you go? Low response rates and the validity of inference in IS questionnaire research. *J. Assoc. Inf. Syst.* **2006**, *7*, 351–414. [CrossRef]
105. Tabachnick, B.G.; Fidell, L.S. *Using Multivariate Statistics*, 4th ed.; Allyn and Bacon: Boston, MA, USA, 2001.
106. Osborne, J.; Waters, E. Four assumptions of multiple regression that researchers should always test, Practical assessment. *Res. Eval.* **2002**, *8*, 1–9.

107. Klockars, A.J.; Sax, G. *Multiple Comparisons*; No. 61; Sage: London, UK, 1986.
108. Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*; Academic Press: New York, NY, USA, 1977.
109. Recker, J. *Scientific Research in Information Systems: A Beginner's Guide*; Springer: Berlin/Heidelberg, Germany, 2012.
110. Baron, R.M.; Kenny, D.A. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *J. Personal. Soc. Psychol.* **1986**, *51*, 1173–1182. [CrossRef]
111. Conger, A.J. A revised definition for suppressor variables: A guide to their identification and interpretation. *Educ. Psychol. Meas.* **1974**, *34*, 35–46. [CrossRef]
112. MacKinnon, D.P.; Krull, J.L.; Lockwood, C.M. Equivalence of the mediation, confounding and suppression effect. *Prev. Sci.* **2000**, *1*, 173–181. [CrossRef] [PubMed]
113. Rucker, D.D.; Preacher, K.J.; Tormala, Z.L.; Petty, R.E. Mediation analysis in social psychology: Current practices and new recommendations. *Soc. Personal. Psychol. Compass* **2011**, *5*, 359–371. [CrossRef]
114. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411–423. [CrossRef]
115. Hair, J.F.; Black, W.C.; Babin, B.J.; Anderson, R.E.; Tatham, R.L. *Multivariate Data Analysis*; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2006.
116. Hooper, D.; Coughlan, J.; Mullen, M. Structural Equation Modelling: Guidelines for Determining Model Fit. *Electron. J. Bus. Res. Methods* **2008**, *6*, 53–60.
117. Darwish, A.; Zarka, A.E.; Aloul, F. Towards Understanding Phishing Victims' Profile. In Proceedings of the International Conference on Computer Systems and Industrial Informatics (ICCSII), Sharjah, UAE, 18–20 December 2012; pp. 1–5.
118. Vishwanath, A. Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *J. Comput. Med. Commun.* **2015**, *20*, 83–98. [CrossRef]
119. Hong, C.; Chen, Z.; Li, C. "Liking" and being "liked": How are personality traits and demographics associated with giving and receiving "likes" on Facebook? *Comput. Hum. Behav.* **2017**, *68*, 292–299. [CrossRef]
120. Lee, E.; Kim, Y.J.; Ahn, J. How do people use Facebook features to manage social capital? *Comput. Hum. Behav.* **2014**, *36*, 440–445. [CrossRef]
121. Burrow, A.L.; Rainone, N. How many likes did I get? Purpose moderates links between positive social media feedback and self-esteem. *J. Exp. Soc. Psychol.* **2017**, *69*, 232–236. [CrossRef]
122. Scissors, L.; Burke, M.; Wengrovitz, S. What's in a Like? Attitudes and Behaviors Around Receiving Likes on Facebook. In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, San Francisco, CA, USA, 27 February–2 March 2016; pp. 1501–1510. [CrossRef]
123. Meshi, D.; Morawetz, C.; Heekeren, H.R. Nucleus accumbens response to gains in reputation for the self relative to gains for others predicts social media use. *Front. Hum. Neurosci.* **2013**, *7*, 1–11. [CrossRef]
124. Cao, J.; Basoglu, K.A.; Sheng, H.; Lowry, P.B. A Systematic Review of Social Networking Research in Information Systems. *Commun. Assoc. Inf. Syst.* **2014**, *36*, 1–41.
125. Twitchell, D.P. Social Engineering in Information Assurance Curricula. In Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 22–23 September 2006; pp. 191–193.
126. Hogben, G. *Security Issues and Recommendations for Online Social Networks*; ENISA Position Paper; European Union Agency for Network and Information Security: Heraklion, Greece, 2007; Volume 1.
127. Baird, C.; Parasnis, G. From social media to social customer relationship management. *IEEE Eng. Manag. Rev.* **2013**, *41*, 48–55. [CrossRef]
128. Dam, J.-W.V.; Michel van de, V. Online profiling and clustering of Facebook users. *Decis. Support Syst.* **2015**, *70*, 60–72.
129. Ngai, E.W.T.; Xiu, L.; Chau, D.C.K. Application of data mining techniques in customer relationship management: A literature review and classification. *Expert Syst. Appl.* **2009**, *36*, 2592–2602. [CrossRef]
130. Park, N.; Lee, S.; Kim, J.H. Individuals' personal network characteristics and patterns of Facebook use: A social network approach. *Comput. Hum. Behav.* **2012**, *28*, 1700–1707. [CrossRef]
131. Erlandsson, F.; Boldt, M.; Johnson, H. Privacy Threats Related to User Profiling in Online Social Networks, Privacy, Security, Risk and Trust (PASSAT). In Proceedings of the 2012 International Conference on Social Computing (SocialCom), Amsterdam, The Netherlands, 3–5 September 2012; pp. 838–842.

132. Wisniewski, P.; Knijnenburg, B.P.; Richter Lipford, H. Profiling Facebook Users' Privacy Behavior. In Proceedings of the SOUPS 2014 Workshop on Privacy Personas and Segmentation, Menlo Park, CA, USA, 9–11 July 2014.
133. Terrana, D.; Augello, A.; Pilato, G. Facebook Users Relationships Analysis Based on Sentiment Classification. In Proceedings of the 2014 IEEE International Conference on Semantic Computing (ICSC), Newport Beach, CA, USA, 16–18 June 2014; pp. 290–296.
134. Terrana, D.; Augello, A.; Pilato, G. A System for Analysis and Comparison of Social Network Profiles. In Proceedings of the 2015 IEEE International Conference on Semantic Computing (ICSC), Anaheim, CA, USA, 7–9 February 2015; pp. 109–115.
135. Nohlberg, M. *Why humans are the weakest link. Social and Human Elements in Information Security: Emerging Trends and Countermeasures*; Gupta, M., Sharman, R., Eds.; IGI Global: Hershey, PA, USA, 2008.
136. D'Arcy, J.; Hovav, A.; Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inf. Syst. Res.* **2009**, *20*, 79–98. [CrossRef]
137. Haney, C.; Banks, C.; Zimbardo, P. *Interpersonal Dynamics in a Simulated Prison*; Defense Technical Information Center: Fort Belvoir, VA, USA, 1972.
138. Mixon, D. Instead of Deception. *J. Theory Soc. Behav.* **1972**, *2*, 145–178. [CrossRef]
139. O'Leary, C.J.; Willis, F.N.; Tomich, E. Conformity under Deceptive and Non-Deceptive Techniques. *Sociol. Q.* **1970**, *11*, 87–93. [CrossRef]
140. Olson, T.; Christiansen, G. *Thirty-One Hours: The Grindstone Experiment*; Canadian Friends Service Committee: Toronto, ON, Canada, 1966.
141. Gibbins, M. Deception: A Tricky Issue for Behavioral Research in Accounting and Auditing. *Auditing* **1992**, *11*, 113.
142. Kimmel, A.J. Deception in Marketing Research and Practice: An Introduction. *Psychol. Market.* **2000**, *18*, 657–661. [CrossRef]
143. Cheung, C.M.; Lee, M.K. What drives consumers to spread electronic word of mouth in online consumer-opinion platforms. *Decis. Support Syst.* **2012**, *53*, 218–225. [CrossRef]
144. Lee, M.K.; Shi, N.; Cheung, C.M.; Lim, K.H.; Sia, C.L. Consumer's decision to shop online: The moderating role of positive informational social influence. *Inf. Manag.* **2011**, *48*, 185–191. [CrossRef]
145. Luo, C.; Luo, X.R.; Schatzberg, L.; Sia, C.L. Impact of informational factors on online recommendation credibility: The moderating role of source credibility. *Decis. Support Syst.* **2013**, *56*, 92–102. [CrossRef]