Source Credibility in Twitter

Ahmad Alturki[1], Ahmad Alsanad[1], Shatha Alhathal[2]

[1] STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia;
[2] Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia;

Corresponding author: Ahmad alturki,

Abstract
Previous research efforts mention that the social engineering illustrates one of the critical security risk/issues. Social engineering considers as the art of deception, manipulation, influencing and deceiving people to force them to perform actions or divulging their confidential information. Recent studies state that Social Networking Sites (SNSs) pose as a breeding ground for social engineering attacks. The danger of social engineering attacks in SNSs is obviously shown in the difficulty of taking accurate judgments about the source credibility in any virtual environment of SNSs. Source credibility is one of the source characteristics which reflects the reliability of that source and therefore, it will influence receivers to accept attacker's message. This research aims to investigate the source credibility concept in terms of social engineering, twitter as an example of SNS, using quantitative approach. The developed model of source credibility judgment for social engineering will contribute in clarifying the main dimensions of source credibility to know how receivers will perceive that source. Moreover, source characteristics that affect twitter's users to make a judgment on the credibility of the attacker.

Keywords: *Source credibility, Twitter, Social networking sites (SNSs), Social engineering, Attacker.*

1. INTRODUCTION

Social networking sites (SNSs) is a virtual community in which users communicate, share and exchanging of all kinds of information. From 1997, when the first recognizable social network site appears (SixDegrees.com), people found this sites attractable to create their profiles and communicate with each other in the way that the site design [1]. Today, SNSs used as a new range of opportunities and as the leading tool for social interaction. People use social networking sites for many purposes; to contact with new and existing friends, use site services in their business, and to exchange knowledge and information. Also, it considers as an invaluable tool for helping people to communicate when there is a natural disaster such as earthquake and Tsunami. For example; in Haiti's earthquake, Twitter has a significant role in updating a real-time basis for it. Haitian's users explained their situation to the whole world, as well as, contact with their families and friends that can't reach them through cell-phone [2].

Social networking sites (SNSs), contain many users and information. Therefore, privacy and security concept are seeming to be essential issues on its environment [3]. These issues occur when a hacker collects information about the victim to discover his weak points. Then, the attacker chooses his plan according to the information that he gathered and based on the goal that he wants to achieve. After that, he attempted to use persuasive skills with his victim to apply the plan [4]. Dimension Research found on its survey which is done on around 850 of the IT and security expert placed in Australia, New Zealand, United Kingdom, Canada, and Germany, on 2011 that 48% of the participants was facing social engineering attack. Moreover, they had an experience with more than 25 attacks in 2010 and 2011. The report also states, that the rate cost that the victims lose on social engineering attacks is around $25,000 to $100,000 per security incident. 39% of the participants think that social networking sites (SNSs) having a suitable environment for social engineering attacks (The risk of social engineering on information security: A survey of IT professionals, 2011).

In order to reduce the significant security risk that comes from social engineering, we investigate the social engineering attacks in its common source, which is the social networking sites (SNSs). The users of SNS may answer the social engineering attack requests and fall as victims because they face difficulty in make an accurate judgment about the source credibility of that request. In this research, we focus specifically on the social engineering attacks on one of the most famous SNS which is Twitter. Quantitative research is done to investigate the source credibility dimensions and its

Manuscript received January 5, 2022
Manuscript revised January 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.1.53

characteristics that will affect in the Twitter user's judgment on the attacker credibility.

Twitter is one of the SNSs with millions of users from all over the world, which start in March of 2006. Using tweet, users can communicate and post 140-character per message. Tweets can be published using e-mails, SMS or directly from smartphones twitter application. Therefore, tweet provides a real-time propagation of information, thus make it an ideal environment to disseminate breaking - news directly from its source and location to users. But Twitter like any others SNSs considers as the perfect source for the attackers to do their plans and tactics which lead a victim into saying "yes" to the trick. Spam, persuasion, and bribery, and lies and misinformation are example attacker's techniques. On January 2011, rumor tweets contain misinformation of shooting in the Oxford Circus in London, and it is spread rapidly via Twitter [5]. CSI/FBI stated in their computer crime and security study, that across 313 companies surveyed, losses of information technology security incidents is about over $52 million [6]. The vulnerabilities of technologies and human have recognized as the most security threaten that facing the information systems. Technology factors are examining and discussed in many studies, but human factors are seeming to be less cover and address by researchers in the information technology field. In general, people are the weakest link under the security perspective. Emotion, feeling and corrupt behaviors of people, or sometimes their failure to comply with the security strategies and the leak of awareness and training on dealing with different security threats are examples of this weakness, and we can consider it, as cues of human vulnerabilities.

Currently, social network sites become a target for several of social engineering attacks. As the Institute of Management and Administration (IOMA) states in 2005, that social engineering is classified as the most critical security risk [7]. Nowadays, SNS users have dramatically increased; according to Statista report, the expected number of overall SNS users around the world in 2018 is about 2.5 billion. Moreover, the amount of sensitive, critical and private information and data of people as well as organizations will increase too. Social engineering is a beneficial way for the attacker to persuade users or force them to do or give him what she/he needs; or trick users to gain information from them. So, Social engineering attacks is a kind of security attack that takes advantages of vulnerabilities to achieve the attacker goal.

Twitter is one of the common social networking sites which used by many users to communicate and share the information with each other over the long distance. However, it also attracts the attackers to use different traps and tactics to achieve what they are looking for. Tweet is the name of the message that a Twitter users use it to communicate. The limitation of tweets size (maximum 140 characters) leads them to share URL of the web pages to get more explanation for the tweet topic. One of the tactics that the attacker used to trick victims is suspicious URLs; she/he attempted to send it in tweets and transfer the users to malicious pages and she/he may get access to their Twitter account [8]. The danger of social engineering attacks in SNSs appears in difficulty for the user to make accurate judgments about the credibility of attackers.

RSA conference and ISACA collaborate to study and give a view about the global status of cyber security and its related issues. Their results show that the types of social engineering attacks are the most common attacks in the enterprises at 2014. The respondents are citing phishing around 70% in company exploitation, and 50% of the result is from the other social engineering attacks. In the United States, around 40% of organizations have banned their employee from using social media to prevent the associated risk with social media. The effect of using the SNSs at work, not only waste time and loss the employee productivity but may influence the organization or networks to become goals for different security threats [9]. On the personal side, many of SNS users attempt to provide their private and sensitive information on their accounts, and this makes them susceptible to various physical and cyber risks [10]. In 2012, the Federal Bureau of Investigation (FBI) states that, when the information posted to a social networking site, it will not become private anymore. Although when the user's account is set as private, hackers can reach these details by employ different techniques.

Several researchers examine the tactics and plan that the attacker follows to attract and reach the victims, for example, Algarni et al. [4] shown the most popular techniques that are used by the attacker in social engineering. Also, Al Hasib [11] list privacy and security threats of SNSs users, as well as he, presents the fundamental factors behind these threats. The future of social engineering risk, especially in SNSs will continue and increase for two reasons. The first, the SNS provider uses some tactics to attract and encourage their users to post more personal information. Then, they will use this information to help them in marketing and advertisements, and therefore, the social engineering exploits will increase. The second one, the SNSs characteristics facilitate the attacker work, for that, it will continue being the fertile soil for social

engineering attacks. (e.g. easy and quick access to the user's account and information) [4].

Security plays a significant role in information systems, to ensure that the main three elements: confidentiality, availability, and integrity of the system have been achieved. Technology vulnerability and human vulnerability can cause a breach, violate and breaking those elements. Many researchers consider people as the weakest link in information security [6, 12]. Humans are fallible by their natures and may face many factors such as time pressure and situational context which might influence their decisions and make them susceptible to exploit. The effect of their weakness is not limited to them, it may be going beyond that to impact their companies, organizations, or even governmental institutions [13]. Statistics said that 70% of information security incidents in many organizations from their employees' behaviors [14]. Moreover, losses of those events may affect the organization profit on approximately 3% [15].

Influencing and tricking people to reaching sensitive information or to do something that will drive benefits for the attacker are called social engineering. Many researchers explain the risk of social engineering in SNSs and they also discuss how social networking sites (SNSs) consider as a breeding ground for social engineering attacks [16, 17]. Social engineering becomes a controversial problem in information security due to the incredible complexity and amazing simplicity of it.

The danger of social engineering attacks in SNSs occurs on the difficulty that facing the users when they attempt to decide and give judgments about the deception in the SNSs environment. The credibility of attackers is an essential element in user view to obeying and refuse social engineering attacks. In general, people are more probably to answer any request if the source shows itself as credible [18]. Source credibility is a multidimensional concept that helps the receiver in his evaluation of the source of information. This assessment associated with the ability of the receiver to recognize the facts, the reality, and truthiness of the received information as well as make accurate judgments of the believability on the source of that information.

This research aims to explore the source credibility dimensions in Twitter context. Moreover, the characteristics of the source that affect Twitter users to judge a decision on the attacker's credibility which leads them to become susceptible to victimization. The result of the current study contributes to the knowledge by producing an explanation theory that explains how source credibility dimensions in case of social engineering on Twitter, and the source characteristics impact the Twitter user's judgment on the credibility of the attacker, which make them susceptive to the victimization. This study improves the model for source credibility judgment in the case of social engineering in Twitter based on Algarni et al. [19] model by adding a new dimension to explain the influence of the message content on source credibility.

The rest of the paper is organized as follows: literature and proposed approach are given in Section II, experiments and discussions are reported in Section III, and finally a conclusion is summarized in Section IV.

2. LITERATURE REVIEW

The literature in this study consists of five parts to cover all aspect of this research. The first subsection discusses the information system theories. Subsection B discuss the source credibility concept in general; which includes three subsections trying to cover the most common fields that involve with source credibility as follow; social media, marketing and online advertising, and in communication and persuasion. The third part, subsection C, explains social engineering and its essential components. The next subsections list some concepts that usually associated with social engineering. The entertainment-education which have been integrated its concept with our research model. The last part talks about a critical instrument which is a questionnaire after giving some details around the method that follow to complete this study which is the quantitative research approach.

A. Information System Theory

Development of good theories in a discipline is a crucial; which is researchers' ultimate objective [20]. "[A] particular kind of model that is intended to account for some subset of phenomena in the real world. … It is an artifact built by humans to achieve some purpose. It is a conceptual thing rather than a concrete thing. Nonetheless, it has a concrete manifestation as a neuronal pattern in some person's brain" [20] (p.4). Theories mean "abstract entities that aim to describe, explain and enhance understanding of the world and, in some cases, to provide predictions of what will happen in the future and to give a basis for intervention and action" [21] (p. 7). In her seminal work, 'The Nature of Theory in Information Systems', Gregor [21] defines four objectives of theories:

- *Analysis and description:* A theory describes; first, phenomena and studies the relationships between the phenomena's constructs; and second, generalizability in these relationships and constructs.
- *Explanation:* A theory describes and explores "how, why and when things happened". It contributes to knowledge of the interesting phenomena.
- *Prediction:* A theory provides an account of "what will happen in the future if certain pre-conditions hold". Such predictions perform an approximated rather than a certain future.
- *Prescription "Recipe":* A theory that is a special case of prediction that provides details such as steps, properties, or structure to construct an artifact.

Based on the previous goals, Gregor [21] identifies five kinds of theories, as shown in Table I. Figure 1, depicts the interrelationships among the theories.

TABLE I. THEORY TYPE IN IS RESEARCH [21].

Theory type	Distinguishing attributes
Analysis	Says "what is". The theory does not extend beyond analysis and description. No causal relationships among phenomena are specified and no predictions are made.
Explanation	Says "what is", "how", "why", "when", "where". The theory provides explanation but does not aim to predict with any precision. There are no testable propositions.
Explanation and Prediction (EP)	Says "what is", "how", "why", "when", "where" and "what will be". It provides predictions and has both testable propositions and causal explanations.
Design and Action	Says "how to do something". The theory gives explicit prescriptions (e.g., methods, techniques, principles of form and function) for constructing an artifact.

B. Source Credibility

Over the past 15 years, according to the International Telecommunication Union (ITU), the Internet user penetration is growing up to seven-fold. Between 2005 and 2019, the global penetration rate increased from nearly 17 per cent to over 53 per cent [22].

With the Internet growth, there is a significant concern about the quality and validity of information that the internet provides. Researchers investigate the credibility of online information; which have been studied by many researchers in different fields, including marketing, psychology, information science and communication.

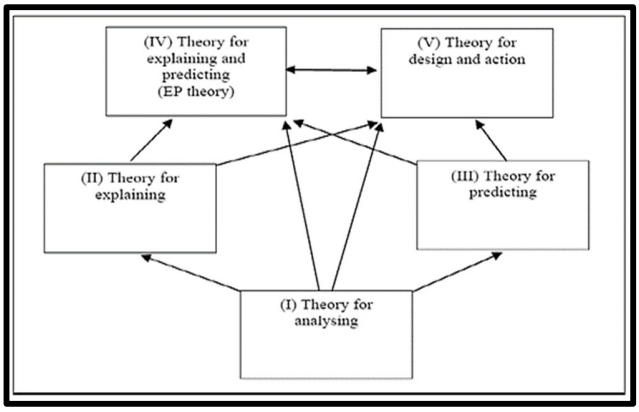

Figure 1. INTERRELATIONSHIPS AMONG THEORY TYPE [21].

For example; scholars study credibility as it has a major role in the persuasion process. In information science, researchers study the credibility as one of the criteria that is used when the users need to make a judgment for

accepting or reject information, (e.g., [23] investigate the news credibility in newspapers, television, and online news media.). Also in marketing, credibility and trust are the based for any successful business.

The concept of credibility was first developed by Aristotle when he has divided the persuasion aspects into three denominations; credibility (ethos), emotion (pathos) and logic (logos) [24]. This means anyone believes what s/he trusts while emotion and logic are the emotional relation and means for dialectics to convince someone on a certain argument [25]. Credibility can be defined using dozens of concepts such as believability, fairness, accuracy, honesty, trust and objectivity. Generally, it is all about the believability of information. In Eisend [26] (p. 2), definesthe credibility as "a person's perception of the truth of a piece of information". The credibility is an "objective and subjective components of the believability of a source or message" [27] (p. 178). "The generalization that high credibility sources are more influential than low credibility sources is as close as one can come to a universal law of persuasion" [28] (p. 89).

IT should be noted that credibility is seen as a multidimensional concept, it varies from one context to another, and it changes over time (dynamic). For example, Gass and Seiter [29] propose three primary dimensions of credibility for persuasive situations; expertise, trustworthiness, and goodwill. The decision-making context on the received message or request depends strongly on degrees of credibility. To assess credibility Hilligoss and Rieh [30] present a unifying framework in three levels to credibility judgments; construct level, heuristics level, and interaction level. First, construct level is an abstract level in which someone can form, conceptualizes and defines credibility. This level contains the credibility notions that affect someone's judgments. Second level, the heuristics; includes standard rules to facilitate making judgments of credibility in all variety of situations. Lastly, the interaction level, make judgments for credibility according to a particular source or cues. In the current study, we call attention on the source credibility to get an accurate judgment on source credibility in the case of Twitter.

Source credibility is "a term commonly used to imply a communicator's positive characteristics that affect the receiver's acceptance of a message" [31] (p. 240). Source credibility is the ability of the message source to provide accurate and honest information [18]. As we mentioned before, persuasion is the root of the source credibility research (by Aristotle). In Hovland et al. [18], the source credibility theory has a propound when the source shows itself as credible, the receivers are more probably to be persuaded and approve his message. This theory is categorized into three parts: the factor model, the functional model, and the constructivist model. The factor model assists in defining the extent of the receiver's judgment on the source credibility. The functional model shows the credibility as degrees to which source gets a receiver's demands. The constructivist model displays the reaction of the receiver to the persuader message. In [32], the authors extend the work of Hovland et al. [18] on their study to examine the standards that the receivers used to evaluate and accept the message sources. This investigation was in three dimensions; safety, qualification, and dynamism. The study by Hovland et al. [18] supports that the source 'image' should be determined by the receiver's perception, not from the source characteristics.

Source credibility have different dimensions, and this become according to varying subject-type or source-type [33]. The most source credibility studies agree that source credibility consists of at least two critical dimensions; source trustworthiness and source expertise which both contribute to the credibility concept [34, 35]. Trustworthiness is an important factor to assess credibility in general. It can be explained that the source trustworthiness as the extent to which a source message appears as reliable, honest and unbiased. However, source expertise are referring to the ability of a source knowledge or expertise to provide accurate, authentic and valid information. While the expertise is influence the capability of the message's source to provide exact information, trustworthiness is seeming to effect a message's source motivation to provide reliable information [36]. Sundar [37] has done an important research in source credibility, and propose MAIN model as depicted in Figure 2. The author examines the technological possibilities that allow to heuristically process cues when people make judgments around the source credibility in an online environment. Based on MAIN model, metrics are used by the system to generate pieces of information. Metrics can be one type of affordance, which can be utilized as positional heuristics to make credibility judgments.

Figure 2. Main disciplines of the source credibility.

It offers heuristic appeals for the people through what this study called it agency cues. Agency cues refer to the cues capitalize on heuristics that privilege credibility cues of computer-generated rather than the one generated by users. Sundar [37] mentions that the people use machine heuristic to investigate online information. Machine heuristic states that people are more likely to assign their credibility to the information that validates or/and selected by machine or computer. Because it cannot think and does not have any emotions or feelings, and therefore their perceived seems to be free from bias. So, this leads to the people to use machines as a source of information rather than human sources such as editors. [38].

Another important study is about Social Information Processing Theory (SIPT) [39], which proposes that any information a channel provides, will help people to make judgments about other people. SIPT theory discusses how things will run with online channels that have a lot of information. SIPT assumes an important thing, which is the online goal of the people are the same to what they do offline. This assumption includes those goals of forming impressions of others. It also suggests that people adapt their perceptions according to information that the channel provides if the channel does not allow to utilize the usual cues [39].

The sections below discuss the main important disciplines of the source credibility as shown in Figure 2, to explain and define the source credibility from different perspectives, and therefore, help us in identity source credibility dimensions in the context of social engineering on Twitter. Furthermore, the characteristics of the source that affect the Twitter users' judgment on an attacker as credible.

1) SOURCE CREDIBILITY IN SOCIAL MEDIA

"Social media is a term used to describe a variety of channels that are built on the idea of collaborative creation and dissemination of content" [40] (p. 199-200). Social media has different platforms in which users can create content and discuss it with others in a collaborative way. Facebook, Twitter, YouTube, Wikipedia, and Flickr are examples of the social media platforms. Social media platforms become part of our live and daily routine; on an individual level, people use them to communicate and entertainment, share information and learning etc.

On organizations level, many of them adopt it as a tool to help in their business, such as get low-cost advertising and marketing, customer relationship management, and online meeting with their vendor and partner.

The content of social media are created by their users; and for this nature, there is an essential demand to judge its credibility. The credibility becomes one of the common concepts that have been studied by many researchers in associated with social media. The "credibility can be suggested as one of the key factors driving the traffic of individuals to organizations' social media" [41] (p. 20). The Credibility is one of the characteristic organizations should care about it on social media to keep their customers, and attract new ones.

Credibility assessment in social media or even in an online environment, in general, are difficult than traditional media. According to Sundar [37], this difficulty is due to the multiplicity of sources embedded in the numerous layers of online dissemination of content. Many researchers discuss and divide the perspectives of online credibility into three dimensions; medium credibility, message/content credibility, and source credibility [42]. Medium credibility is perceived about the credibility level on a particular medium that

individual users have like the one about specific such as blogs, or newspapers. Message credibility concerns about the communicated message credibility; e.g. accuracy, quality, and currency of the information that the message has. Source credibility is about making a judgment about the credibility of the source; which effects on the acceptance of the transmitted message to the receiver. Due to the goal of this research, the focus will be on the last one, source credibility, to find the characteristics of the source which leads the Twitter user to judge an attacker as credible.

Algarni et al. [43] predict human's vulnerability in social engineering according to demographic factors such as age, and gender. They examined the characteristics of the source that lead Facebook users to judgment on the credibility of the attacker. Algarni et al. [43] employed mixed methods which start with a qualitative phase using grounded theory method to develop their model, and then they conducted a quantitative method in [19]. They used multiple sources; one observes Facebook profiles and timelines, and in-depth interviews. The research model includes perceived sincerity, perceived competence, and perceived attraction; these three dimensions are reported in communication and marketing research. The last dimension of the model is perceived worthiness which is the outcome of the qualitative phase. Authors define 13 source characteristics, and they are distributed as follows: perceived sincerity includes: 1) number of friends, 2) common friends, 3) number of posts, 4) common beliefs, and 5) real name.; for perceived competence contains: 6) qualifications, 7) celebrity, 8) wealth; for perceived attraction there are: 9) good looks, 10) good writing skills; and for perceived worthiness includes: 11) authority, 12) sexual compatibility, and 13) reciprocity. While Algarni et al. [44] use a qualitative questionnaire-based survey in the qualitative phase to gather and analyses the experiences of the people with attacks of SNSs or with social engineering tricks and deceptions. Algarni et al. [19] implement quantitative phase to investigate the dimensions of source credibility in social engineering on Facebook, and the characteristics of the source that led Facebook users to judgment on the credibility of the attacker. With a role-play experiment, the authors examine the of source characteristics under a various demographic category by measuring the user's consent intentions and their behavior responses to SE requests to be able to predict based on their demographics if they were susceptive to social engineering victimization.

The results show that all factors in the source credibility dimensions are significant predictors of susceptibility to SE victimization. The most dimension that affects the user judgment on the attack request on Facebook is perceived sincerity followed by perceived worthiness, then perceived competence, lastly perceived attraction. The results classify the source characteristics according to its impact on each dimension. For perceived sincerity is 1) number of friends, 2) the source's use of a real name, 3) common friends, 4) number of posts, and 5) common beliefs. For the perceived competence: 1) celebrity, 2) qualifications (educational level), and 3) wealth. For the perceived attraction: 1) good looks and 2) good writing skills. The last one for perceived worthiness 1) authority, 2) sexual compatibility and 3) reciprocity. Finally, the result show that there is variance in perceptions and behaviors of the demographic groups to social engineering requests.

1.1) TWITTER

Twitter, a micro-blogging service that connects 1.3 billion accounts and 336 million active users from all over the world [45]. Twitter has seen a lot of growth since it launched in March of 2006 [46]. Twitter is considered as one of common social network sites. Twitter attracts a lot of users due to its ease of use and sharing real-time information with a large group of users. It differs from other online SNS like Facebook or MySpace; Kwak et al. [47] stated that no reciprocation required in the relationship of following and being followed. Therefore, when the user follows any other user, the other user is free and doesn't need to follow him back. Twitter is focused on linking topics, while for example, Facebook is focused on linking people. While Facebook usually connects users with their friends and relatives, Twitter connects users with anyone.

Being a user follower in Twitter means that s/he will receive all the messages from other users that s/he follows. Twitter's message or tweets consist of 140 characters and this restriction make users use a well-defined markup culture such as 'RT' stands for retweet, and '@' to identify the user address [48]. A retweet mechanism in Twitter is a simple, yet powerful way for users to spread information on the Twitter social network which make it an ideal environment to dissemination the knowledge and news [49]; and at the same time susceptible to social engineering attacks. It should be noted that participants in Algarni et al.'s study [44] classify Twitter as the second type of SNS after Facebook.

There are factors that affect the source credibility on Twitter. Many studies focused on social media as a source of information and news (include information regarding of crisis and dangers), which leads to important questions, are that information credible and how people can give a judgment about the credibility of

the information source. Castillo et al. [5] analyzed the credibility news that are propagated on the Twitter throw using the method to assessing the credibility on a set of given tweets. First, they analyzed the trending topics of the postings and classify the post as credible or not credible based on features (message, a user, a topic, and propagation- based features). After that, they evaluated the methods on a recent sample of Twitter postings. Finally, they asked the evaluators to assessment the credibility. The research proposed by Castillo et al. [50] developed two classifiers for a testing how well these two classifiers (newsworthy event, credibility) transmitted over a natural disaster to Twitter topics in Spanish. Gupta and Kumaraguru [51] assessed the credibility of information in tweets level based on different news events. They found that highest tweets post is about the event situational information with an average of 30%. Then, 17% found to be credible, and it was about situational awareness information, and 14% was for spam. They used regression analysis to predict the credibility of information in a tweet based on the features of content (e.g. emoticons and number of pronouns) and source (e.g. number of followers). In addition, they present ranking algorithm using Twitter features to evaluate the information credibility in tweets. Many researchers build their research using system generated cues (which is pieces of information the system often generated and rendered based on a user's behavior on that system) [52]. Because it's as what Sundar [37] states, shows to be a reliable indicator and important determinants to underlying construct and for the judgments of the source (like its credibility). Believing that the machines never lie, information provided by system seems to be reliable and credible (e.g. Number of friends on Facebook). Westerman et al. [40] examine how information (the number of followers, the ratio of followers to follows) on three-dimensional competences, trustworthiness and goodwill affect the judgments of the source credibility on Twitter. The results show that the number of followers affects trustworthiness and competence; and the ratio of followers to follows lead to growing judgments of competence. That is, if the account owner has a lot of followers, but he follows a few people, s/he is considered as less of an expert.

Later, Westerman et al. [46] study the effect after exposure to the page, the speed (recency) on the page of social media had on the source credibility judgments and cognitive elaboration. Participants were asked to view one of three Twitter pages that differ the recency with which tweets were posted. After that, evaluated measures source credibility and cognitive elaboration. The result shows that recency of updates affect cognitive elaboration and therefore, which impacted source credibility.

The work presented by Sikdar et al. [53], explain a new method of constructing microblogging sites reliable and significant credibility ground truth values such as Twitter in individual message level. Sikdar et al. [53] show that there is a different on the survey's results and can be affected by some frames on the survey's questions. Prediction of retweet behavior with network-based features is an easy task, but this task may be differ from a network to another, giving different information about credibility. To state these two measures, Sikdar et al. [53] conduct a credibility study (in different network characteristics) on two various data sets of the same subject, and also on two of users' surveys. Depending on the retweet behavior, they structured two further credibility indicators and formulated their finding to be that the ground truth must be carefully defined and measured based on any credibility study. On another hand, [54] investigated how two main microblogging features (the author's credential and microblog reply) can help the user's evaluation of the credibility of health advice on different health topics.

To know more about people behave on Twitter, Counts and Fisher [55] discuss what information in a microblog stream is attended to the user, and how the attention and their reaction will be. To do this, they examine the Twitter users when they read their tweet streams by tracking their eyes, measured their interest and memory for the content and observe the reaction they take. The results show that the user takes around three seconds in reading each tweet and may use it to attend to content they find interesting and remember. User reaction (replies, retweets) are taken for highly interesting content.

2) SOURCE CREDIBILITY IN MARKETING AND ONLINE ADVERTISING

Marketing is an important concept to success any business; it is a heart of any business. The company might have a good product, but it forced to close because it not known for the target customer. Marketing refers to the process of preparing the product or service to be suitable for the marketplace [56]. Advertising considered as one of the essential components of the marketing process. The advertising is as a process that allows the company's product or service to become known to potential customers [57]. There are different channels to reach those target audiences such as newspapers, television, radio, and the most important one is the Internet. According to Bayer et al. [58], the IAB Internet advertising revenue report issued in 2019 stated that the revenues of the United States from online

advertising exceeding $100 billion in 2018, giving a clear figure about the impact of the internet advertising on the revenues of the countries.

In marketing and advertising field, customers really concern the credibility of the source information of product or service. Organizations, or their representatives, are the sources of the information while the receiver are their customers. So, the source credibility can be defined as judgments that the user can make about the believability, truthful and the accurate of the source information, and the confidence degree that the receiver has to the source of the message [59]. The work of MacKenzie and Lutz [60] defin the credibility in the context of advertising as "consumer's perceptions of the truthfulness and believability of advertising in general" (p. 51).

There are different factors that affect the judgment of the consumer toward the advertising credibility in an online environment [61]. For example, the corporate has high credibility and trustworthiness (organization experience and its name in the marketplace), the advertiser that can be appeared as credible or sometimes in the design (have a logo, colors, graphics, etc.), and the placement of the advertisement on the online page. Moreover, the attitudes of females differs from males, and receivers' education level and knowledge, and the demographic variables make different effects on the response toward advertisements. Psychological factors like thoughts, sensations, and feelings, have major correlation and effects in online advertising with a customer's experience [62].

Eisend [26], in his influential study, examines whether the existent in marketing communication can generalize the source of credibility concept. The author re-analysis previous studies of the source credibility concept to extract and develops a rigorous measure of source credibility in marketing communication. For that, the author performs an analysis procedure in different steps to get reliable and validated results. The results show three main dimensions of source credibility in marketing communication; which are the tendency toward truth, the possibility of truth, and the presentation.

Regarding source credibility in the online advertisement Nan [63] in his study examines the impact of perceived source credibility on advertising persuasiveness based on two factors. The first factor includes two cases: the identification time of the source before the message exposure, and the identification time of the source after the message exposure. The second factor explores the psychological processes on the advertising persuasiveness. The results of Nan [63] study show that the effect change (in perceived source credibility on persuasion) for persons with low needs before message exposure is stronger than after message exposure. Moreover, the time for source identification does not affect individuals with high needs

The source and advertising are two cues that people may rely on when they make a judgment on online information. So, Greer [64] isolates them and examines if they used by web users. In an experimental design, an online news story displayed for the participants in high or low Web source credibility, enclosed by advertising in high- or low-credibility. He formulates a hypothesis; participants will search for surrounding advertising as another cue if the brand-name news source not appears. Advertising credibility was not attached by the participants' ranking of the story while source credibility has significantly tied. Ads have little effect on the participant's attention, although when it covers one-third of the web page.

Verma et al. [65]divide research of source credibility in advertising into advertiser/corporate credibility and endorser/celebrity credibility. They mention that the endorser/celebrity credibility is based on two models; The source credibility model proposed in Hovland et al. [18] which involves two trustworthiness and expertise dimensions. The second model is source attractiveness model proposed by McGuire and Physics [66], the respondents on the effectiveness of a message will be according to the source familiarity, likeability, and attractiveness. For expertise, trustworthiness and attractiveness dimensions, Ohanian [31] develops a measurement for the source credibility. Other researchers [67, 68] focus on the advertiser or corporate credibility; which is the consumer's belief and trust towards the corporate ability in satisfying its needs in terms of expertise and trustworthiness.

3) SOURCE CREDIBILITY IN COMMUNICATION AND PERSUASION

Transfer information from one to another is known as communication; which has many types [69]. Communication can be verbal communication using sounds and language (Speech) to transfer a message. Not-verbal communication is without words such as facial expressions, or body language. Written communication is another type referring to the interaction caused by written word either printed or handwritten such as e-mail, or e-chatting. 'To communication' is a simple definition of communication, but the definition might differ based on the communication process that a person should go through. The communication process consists of a set of sequential steps which start when a sender (source)

attempts to transfer a message through a communication channel to the receiver, and then a receiver decodes the message and deliver his/her response to the sender [70].

Source credibility is a concept commonly used to give a communicator's positive feature to influence a receiver toward accepting the message [31]. The source credibility model is a collaborative landmark study of Hovland et al. [18]. They analyze the factors that influence the credibility of the communicator, and they found that the expertise and trustworthiness are two factors underscore the concept of source credibility. Expertise is about the source perceived the ability to provide valid assertions, which is in our communication context, the extent to which the communicator can give accurate and valid information, or s/he can examine and discuss a specific subject. The trustworthiness is the perceived readiness of the source to provide adequate assertions, in a communication setting, it is an audience's belief and feeling about the honest of information, reliable and fair that provided by the communicator. So, the source credibility model confirms that the credibility of a transferred message is a recipient's perception task of trustworthiness of the message's source. Simply stated, the recipient will accept and find a message credible only if he perceives the sender to be trustworthy.

Many studies discuss source credibility in a communication area, such as [71, 72]; where they attempt to measure the source credibility of instructor's speech communication (teacher). McCroskey et al. [72] show that the teacher-credibility instrument that was improved is a reliable measure; has satisfying face validity and predictive validity. The instrument is probably useful to the speech communication instructor for the goal which is teacher evaluation in the case, standardized, criterion based measures of student learning are not workable. While Hewgill and Miller [73] seek to study source credibility in response to the fear - arousing communications. They find mild feel appeals are less effective than high fear appeals, and this may appear if the speaker's credibility is high as well as if the threat is made not to the receiver only but also to the receiver's family. For that, they prepared a message directing fear to family members. They discover high fear appeals are more effective in producing attitude change for the high credibility speaker than low fear appeals. Therefore, the source credibility is a serious element to success an emotional appeal.

Other studies state that if the source is perceived as more credible, the influence of the delivered persuasive communication will be greater (e.g. [65, 74]). Persuasive is considered as a factor/ concept to success any communication. Persuasively refers to human communication that aims to influence a person's beliefs, motivations, values, behaviors or attitudes [75]. The persuasive on communication includes five components; message, channel, source, receiver, and destination variables. The source variables involve three essential parts; credibility, attractiveness, and power [66]. Our focus here is source credibility in persuasive.

The persuasive influences source credibility; the highly credible spokespeople have more persuasion toward the advocacy than do communicators with less credibility [18, 76]. The source credibility dimensions, trustworthiness and expertise, have a different perspective in persuasive studies. For example, McGinnies and Ward [77] state that the communicator with trustworthy feature has more influential than an untrustworthy one, whatever s/he is an expert or not. While other studies have another opinion, the audience is judged on the source who profited from persuading as less effect and might provide less attitude change, but their judgment variance if the source was an expert as well [18, 78]. Jain and Posavac [79] study show that the source that has high credible might be utilized to make experience claims more persuasive.

The effect of identification's time of the source is examined to see if the source seems to be highly credible at the begging of the message or in the middle, it will appear to be more persuasive from the identifying it at the end [80, 81]. Ward and McGinnies [82] find that a highly credible source performs better than a low credible one when the identification is known before the message but when identification is delayed the source doesn't affect. In Wegner et al. [83], investigate the influence of source credibility and media innuendos on the impressions of the audience on the innuendo targets. They found that there is less influence on the persuasiveness of innuendos, although diversity in source credibility affects the persuasiveness of direct incriminating assertions. Resulting that the message style affects the source credibility effectiveness.

The Elaboration Likelihood Model (ELM) [84-86] is one of the most concludes models in persuasion. ELM is a dual process theory for explaining the change of attitudes form. The model is considered as a general framework for planning, understanding, and organizing the influencing of the persuasive in communications. The goal of this model is to describe multiple ways of processing stimuli, the reasons for the used and outcomes in attitude change. ELM have proposed in two types of routes; the central/cue route and the peripheral route; and under these two divisions all different theories of attitude change can be addressed/mapped. In

the cue route, attitudes changed by accurate evaluation of the information presented in the attitude issue or object. While in the peripheral route, attitudes are changed by combines the object with either positive or negative cue or by utilizing cognitive shortcuts without active thinking about the object and its attributes [84-86]. In the ELM, there are many variables that affect the important variables in the persuasive process and the characteristics of the source (e.g. credibility), presenting the argument. Under the elaboration likelihood, if the receiving information released from the credible source is low, it will be influenced by the acceptance of the information [87].

C) Social Engineering

Social engineering is about deceiving people to detect and occupy their critical information or forcing them to perform what the attacker need to achieve his goal [88]. As we mentioned before, social engineering plays an important role in threatening and attacks most security defenses whether on people, organizations, companies, or an even insensitive institution like for governments. Social engineering has some tactics to deceptive people in information technology by utilizing websites, e-mails, and social networks to trick them and leads to falling victim to different attacks and crimes like phishing, identity theft, financial abuse, etc. [89].
Social engineering threats in SNSs consist of several entities [90]. First one is the environment or the social networking sites. Social networking sites have two ways that affect the success of social engineering attacks; collect information around the victims to find their vulnerabilities, and direct reaches the victim. The second entity is the social engineer (attacker) who starts by understanding the targeted victim; develops a suitable trick; and then concludes by launching plan and achieve the goal. The third one is the plan and technique (trick); the social engineer should prepare a perfect plan and technique to succeed in achieving the goal, the plan may involve time, resources, and steps to be followed. Techniques include many different forms such as spam, phishing and persuasion and bribery. The last entity one is the victims or SNS users; a person who directly deals with a trick and fall victim to social engineering attacks [4].

In the sections below we want to get more understanding of social engineering and human behavior under threat (what and how they do, accept and failing on it) in different conditions as follow:

1) TRUST

Trust in a comprehensive view; it is a commitment or responsibilities that someone/something imposed to do toward whom confidence or reliance is placed [91]. The trust consists of two-act; emotional and logical. Emotional is where a person exposes his/her vulnerabilities to the others, but he believes that will not take advantage of his/her openness. The logical where the person evaluates chances of earning and loss, calculating according to hard performance data the expected utility and then concluded that the person would conduct in a predictable manner. Social engineers may use different tricks to deceive users that they trust and even s/he may communicate with a victim to gain confidence. For instance, it is much easier for a social engineer to trick the victim to get his password rather than hacking his account. Another example, it could be through e-mail when social engineer presents himself as fake legitimacy (e.g. bank), and requests for verifying some information, the victim trusts and answer his/her demand.

2) DECEPTION

In general, deception is about hiding the truth, especially to get any benefit. Even though, research studies state that people have weakness and really bad in detecting deception, people thought that they are really smart in detecting deception. [92]. This tactic work because people are helpful in their nature and these human characteristics assist the social engineering attacker in deceiving them and achieving his goal. For example, the social engineer may use the personal information that presents in SNS like Facebook to pose as acquaintance or business associate for reaching to critical information.

3) PERSUASION

Persuasion is discussed and mentioned before; which concluding that the speaker's credibility has a major role in persuading audiences [78]. Algarni et al. [4] lists the different persuasion tactics that social engineer using it to trick victims such as scarcity, which is used to push the victim to make faster respond and accept their trap. Likeness is another trick; where social engineer tends to be like another one for charming, attractive or because s/he is one of the celebrities. Social engineers exploit users fund to attract them to obey what s/he wants to do. Authority as a trick; people tend to say yes and compliance to the others who have power.

4) MANIPULATION

The manipulation in social engineering can be defined as a person who skillful and expert in create a false or misleading appearance to deceive [93]. Algarni et al. [94] describe the similarity between manipulation and persuasion as follow; both consist of three factors; the sender (source), the message, and the recipient. Attackers in manipulation and persuasion use brain and

emotion to accept the message, as well as, sender credibility has an important role. Algarni [44] also depicts the difference between manipulation and persuasion, while in persuasion recipients are free to believe and accept the arguments of the persuader (sender), in manipulation the recipients incapable to know manipulator real intentions or to see the consequences of beliefs manipulators trap. The social engineering attack may employ emotional and persuasion to manipulate the victims to make him obey. For example, the social engineer may impersonate victim's friend character that s/he trusts, to manipulate the victim and get access to her/his information.

5) EXPLOITATION

Exploitation is the act of use something or treating people unfairly in order to get an advantage from them [95]. Algarni et al. [43] mention story of about participant's friend exploiting experience, she knows someone through Facebook who introduced himself as a rich person. After a while, she trusts him after chatting him on Facebook. Once, he told her that he faces trouble in his business and he wants to borrow some money from her. Regrettably, after he takes the money, directly he removed her from a friend list and disappeared. In this story, the victim is not only exposure to the physical abuse, but to emotional exploitation and this will lead to broken her trust in anyone of her friends.

D) Entertainment Education

Entertainment education or edutainment is an effective way to inform people about a social issues or concerns, and bring about social change. The entertainment-education (E-E) is a strategy to enclose the education message in entertainment content to increase awareness, knowledge or even change behavior towards the particular educational issue [96]. This policy has been implemented in television, games, and radio. Entertainment-education started in radio in 1951 with The Archers, while on television in 1969 [97]. Moyer-Gusé [98] discusses the persuasive impacts of E-E messages in order to achieve three objectives. First, examines the viewers' involvement with a story itself and how they follow the events develop in the story. Moreover, Involvement with characters and its different related constructs which is; identification (the viewer emotional and cognitive process that he takes based on the character role in a narrative), wishful identification (viewer hope to be like the character), parasocial interaction (PSI) (refer to the audience member interaction with media), similarity (audience desire to be similar to the character) and liking (character positive evaluations). Secondly, she discusses the two main theories that addressed entertainment education message processing to exert persuasive influences by overcoming resistance; social cognitive theory and an extended elaboration likelihood model. Finally, based on the previous theories, she expanded a theoretical framework in order to investigate how each type of involvement assist in cope resistance, concluding in persuasive impacts.

The work [98] called on her study for needed to further research to cover the procedures in which cognitive processes (narrative and characters involvement) provide entertainment-education impacts. In response to that, [99] examined how three constructs which are; involvement with a specific character, with the narrative and viewers' reaction to the narrative. Using a pretest/posttest survey of 167 viewers, the best predictor of change in relevant knowledge, attitudes, and behavior was transportation or involvement with the narrative. Although involvement with a particular character has been hailed as one of the most critical direct predictors of entertainment-education effects, a structural equation model state that sources as with a particular character may affect the heighten of transportation and emotion, therefore, result in changing viewers' knowledge, attitudes, and behavior.

III. RESEARCH METHODOLOGY

The quantitative research is employed in the current study to examine the dimensions of source credibility in case of social engineering on Twitter. Specifically, what the source characteristics that impact Twitter users' judgment on the credibility of the attacker, and which of them make susceptive to the victimization. The research questions are:

- **RQ1:** *What are the dimensions of source credibility in terms of social engineering in Twitter?*
- **RQ2:** *What are the characteristics of the source that affect the Twitter user's judgment on the credibility of the attacker? Which make them susceptive to the victimization!*

A) Exploring and Forming Source Credibility Dimensions in Terms of Social Engineering

From the previous literature, we can observe that the source credibility is a multidimensional concept, and these dimensions differ based on the subject and source type [33]. Source credibility in general consist of two main dimensions; trustworthiness and expertise/competence [34, 35]. Conducted literature, review mentioned above, shows the source credibility dimensions are: in social media, trustworthiness, expertise/competence, and goodwill [40, 46]. In marketing and online advertising some studies mention two dimensions; trustworthiness and expertise (e.g. [63, 64]); however, Eisend [26] re-analysis previous studies

in order to generalize a source credibility concept in marketing communication concluding with three main dimensions which are the trustworthiness, expertise, and attraction. Finally, in communication and persuasion, Hovland et al. [18] place the foundation of the source credibility dimensions on which are trustworthiness and expertise. However, source credibility dimensions improve by Ohanian [31] to encompass the attraction as well. Consequently, we can perceive that most researchers in a source credibility area have agreed on three primly dimensions which are trustworthiness, expertise/competence, and attraction/goodwill. Several research studies in social media often use these dimensions to get accurate judgment around the owner of the account [19, 40, 46]. For that, in this study, the trustworthiness, competence, and attraction dimensions will be examined in Twitter context, to investigate how users can make an accurate judgment on the source credibility.

Trustworthiness dimension, or sincerity for more general, is defined as how users or a victim perceives the source as honest, trusted, believable and unbiased. When users perceived the source as sincerity, they will feel that source is safety and free from danger and then attacks will not be discovered [19]. Expertise or competence of the source means having a required ability, knowledge, and skills or any other special characteristic. Algarni et al. [19], discuss how the competence has a great relationship with trust (a competency account perceived as a trusted source for the user and then it will affect his judgment on that source) and the impact of that relation in marketing and advertisement, information systems and educational level. Competence is also studied in communication along with instructors (teacher) communication in education poses [71, 72]. So, if the source perceives as competence, the Twitter user will trust and accept a message. Similar to the students in the education process, when they accept any information from their qualified teacher, because they believe in whatever he says. The third dimension that may influence Twitter users to assess on others as credible is source's attraction. Attraction means a characteristic or quality that evokes the feeling of liking, interest, and enjoyable. The attraction has a great relationship with likeability; that is if someone like a person s/he will tend to do what someone wants [19]. The attractiveness model states that the source familiarity, likability, and attractiveness will influence the respondents toward the effectiveness of a message [66]. Sincerity, Competence, and Attraction are the first three dimensions that we will be included in our prior model. Hypothesizes are as the following:

Ha1: *User probability of falling as the victim in social engineering is positively related with perceived source as sincerity.*
Ha2: *User probability of falling as the victim in social engineering is positively related with perceived source as competence.*
Ha3: *User probability of falling as the victim in social engineering is positively related with perceived source as an attraction.*

The new dimension that we want to add is the reliability which is the degree to which the receiver perceives the source as dependable based on its message's characteristics. E-E is a strategic process that is designed and implemented on a media message to entertain and educate to increase knowledge about an educational issue and facilitating pro-social change [98]. Therefore, the entertainment content on the educational message will influence to persuasion the receiver and delivers the message [97, 98]. The message content in a Twitter setting will influence on persuasion the receiver and show the source as credible. So, we can hypothesize the following:
Ha4: *User probability of falling as a victim for social engineering is positively related with perceived source as reliable.*

B) Define the source characteristics that affect the Twitter user's judgment on an attacker as credible:

For the first dimension sincerity, Algarni et al. [19] mention that the number of friends, the number of posts, a common friend, common beliefs, and real name are factors which affect when a Facebook user's judging on sincerity dimension. Analogy, in Twitter context, source characteristics related to sincerity are: a content interaction which means the interaction of the source in SNS environments. Social information processing theory (SIPT) suggests that whatever information that the channel provides are used by people to make judgments about other people [39]. These interactions are considering as one of that information, and it will be on Twitter sitting; a number of tweets, multimedia, and likes. As the interaction increase, users may guarantee that the account is not fake and they will perceive it as sincerity. authors The main model in [37] is about the machine heuristic which suggests that the information that is checked or creates by a machine or computer is seen more credible by the people. A number of followers are generating by Twitter and its help in make judgments on the source as sincerity because it also follows and judges by others as credible, and this credibility effect by their numbers. Bio description or biography, it is a curriculum vitae ,or it is a set of words a user typed in a dedicated place in the SNS to give a

clear picture of himself. Users may share beliefs, specialize, habits, interest, or any other things with the source as the Bio show, which leads them to accept any message that comes from it. Having a real name and real picture in the account at the same time, some people consider it as evidence of the sincerity of the source and their desire to find new friends, exchange knowledge, and achieve the social networking site goal, which is the effective communication between community members. The last factor is common followers when the user sees that the source of the message has common followers with him, this encourages him to accept his request because he trusts what the others judge on that source. Therefore, the hypotheses are as following:

Hb1: As the amount of source's content interaction increases, a perceiver's judgment about the source's credibility in a term of sincerity increases.

Hb2: As the source's number of followers' increases, a perceiver's judgment about the source's credibility in a term of sincerity increases.

Hb3: Sharing common interests are positively related to perceiver's judgment about the source's credibility in a term of sincerity.

Hb4: Having a real name and picture of the source is positively related to perceiver's judgment about the source's credibility in a term of sincerity.

Hb5: As the number of the source's common followers' increases, a perceiver's judgment about the source's credibility in a term of sincerity increases.

Secondly, Algarni [44] discussed the factors that affect the competence dimension, which is a celebrity, wealth, and qualifications of the people. These characteristics may lead Facebook users to trust the source who have them and do anything to get some attention or contact with him. Social engineers can use this point to deceit the victim and achieve his/her goal while the victim thought that s/he communicates with the right person [19]. Westerman et al. [40], address the effect regarding the ratio of the number of followers to the number of follows on the credibility judgment and its role in showing source as an expert . Thus, we can suggest that the factors that influence users to perceived source as competence are the celebrity, richness, qualifications, and the ratio of followers to follows. Hence, we can suggest the following hypotheses:

Hb6: The source's celebrity is positively related to perceiver's judgment about the source's credibility in a term of competence.

Hb7: The richness of the source is positively related to perceiver's judgment about the source's credibility in a term of competence.

Hb8: The qualifications of the source are positively related to perceiver's judgment about the source's credibility in a term of competence.

Hb9: The ratio of followers' number to follows is positively related to perceiver's judgment about the source's credibility in a term of competence.

For the attraction, third dimension, the factors that affect perceiving the source as attraction are good looks and good writing skills [19]. Good appearance in Twitter is referred to how the source designs his/her profile to become wonderful and attractive. Some of Twitter's users attempt to customized their account by selecting or adding an amazing picture for his/her header photo and profile photo, change their theme color and modify background image position, color or upload a new one, in order to make their account distinctive and attractive. Victims may accept a message when they see that the source of that message is wondrous. Good writing skills is another factor that attracts victims to answer a message because s/he admires and likes the way of wording and fantastic writing that the source has. The hypotheses for attraction dimension are:

Hb10: The source's good appearance is positively related to perceiver's judgment about the source's credibility in term of attraction.

Hb11: The good writing skills that the source has are positively related to perceiver's judgment about the source's credibility in term of attraction.

For the last dimension which is reliability, the first factor is message style. The Entertainment education message has a different manner to construct it to ensure successful deliver the message to audiences. As Murphy et al. [99] mention about three mechanisms that are frequently cited in construct the message which is involvement with a particular character, involvement with the narrative and viewers' emotional reaction to the narrative. Similar to the message in the Twitter context, the social engineer employs different styles on the message to deceive the victim. To do that, s/he chose the proper style for a victim after examining victim's situation and gathers information around the victim [4]. A message style could be emotional, political or even information about a celebrity that a victim prefers. The second factor is the interaction of the content which refers to a number of likes or retweet on the message content (tweet). The work Counts and Fisher [55] examine the attention that users pay in their Twitter's timeline. Eye-tracking techniques were used to measure which tweets has more user's attention. Among their findings, retweets are one of the tweet characteristics that reflects the user's attention and interest. A high number of retweet may attract user attention on the tweet content and therefore it will increase the trust and

credibility feeling through that source [54]. Social engineers may use many techniques or may pay money to increase their number of retweet. Therefore, the tweet will contain a high number of retweet, and then victims will think that the source is credible. The last factor is the message content, which refers to the message content itself since it has a critical role in determining credibility. The tweet or a message, in general, will perceive as more credible if it contains information that associated with URLs (including news picture (e.g. newspaper snips), video or resource) [51]. Consequently, the reliability of the source will increase. Hypothesizes of this dimension are:

Hb12: Message style is positively related to perceiver's judgment about the source's credibility in a term of the source's reliability.

Hb13: As the interaction of the message content increases, a perceiver's judgment about the source's credibility in a term of reliability increases.

Hb14: The source's message content is positively related to perceiver's judgment about the source's credibility in term of reliability.

.

Figure 3 depicts the proposed priori model showing four dimensions (sincerity, competence, attraction, and reliability) and their fourteen source characteristics. Sincerity is about the degree to which the users will perceive the honest, trusted, believable and unbiased of the source. This dimension involves five characteristics; 1) Content interaction, 2) Number of followers, 3) Common interests, 4) Having real name and picture, and 5) Common followers. Competence is the degree to which the source has the required ability, knowledge, and skills or any other special characteristic. Competence dimension has four components; 1) Celebrity, 2) Richness, 3) Qualifications, 4) Ratio of followers to follows. Attraction means the degree to which a source has the characteristic that evokes the feeling of liking, interest, enjoyable. The attraction includes two properties; 1) Good appearance and 2) Good writing skills. The last one is reliability which is the degree to which the receiver perceives the source based on its message's characteristics. The reliability dimension includes; 1) Message style, and 2) Message content interaction, 3) Message content

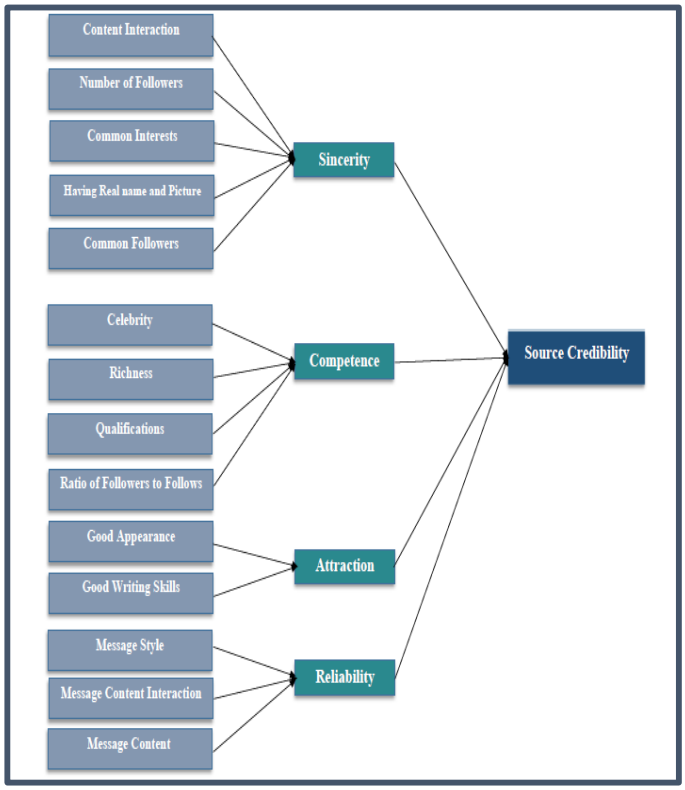

Figure 3. PROPOSED MODEL OF SOURCE CREDIBILITY IN TERMS OF SOCIAL ENGINEERING IN TWITTER.

3. EXPERIMENT DESIGN

A) Method

Quasi-experimental design is used in this research because it has multiple levels of measurement (source credibility dimensions). In the research questionnaire, Role - Play experiment is implemented to test the hypotheses as it is clarified in the next section. To manipulate the research variables; the fractional factorial design method is used to reduce the experimental costs and effort. After that, the scales is developed and test for each dimension items to get a reliable result. The approach and procedures of this experiment are explained as follow.

1) ROLE-PLAY (SCENARIO-BASED) EXPERIMENT

The Oxford English Dictionary explains the role-play as "Noun the acting out of a particular role, either consciously (as a technique in psychotherapy or training) or unconsciously (in accordance with the perceived expectations of society)" [100]. Role-play is considered as a powerful technique across multiple fields; role-play simulation (it is experiential learning method where role players tend to interact towards a particular normative pattern) [101]. Role-play in education (it is a learning structure that helps students to explore and learn from taking a role and interacting with others to improve their experience and trial different situations [102]. Moreover, role-play in entertainment (Role-Playing Games (RPG) it is a game where the player conduct the role of characters within a narrative in a fictional environment) [103]. Yardley-Matwiejczuk [104] give a great deal about role-play literature in the psychology context, specifically in occupational and organizational training, in clinical (therapy and treatment), and in research orientated (explore how people behave under a particular situation).Experimental design determines how participants are assigned to various situations in an experiment. A Scenario-Based Role-Play experiments (SBRP experiment) is a type of experimental design, where researchers use it to test their hypotheses to get an answer to their research questions. The Role-Play experiment is a technique commonly used to study the interpersonal behavior of the research participants by giving them pictures, scenario or any examples based on real-life situations [105]. The Role-Play experiment technique has served many studies in the information security domain. For example, in phishing e-mail studies the researchers use it in displaying different images for many e-mails to the participants and then clarify how they will react if they receive these e-mails (e.g. [106], [107]). Also, it is used to measure the credibility in Social Network Sites (SNS) by present various profiles to the participants and then ask them to rate the credibility on such profile; like in Facebook [19] and Twitter [40].

In this study, a Role-Play experimental questionnaire is conducted by display different Twitter profiles for the participants and ask them to give their rate for each profile according to its characteristics which are the manipulated variables that we want to test it. Every profile has a scenario to clarify some information of the profile's owner (source) that allow the participants to get a clear perception around the characteristics under study. A 7-point semantic differential scale is used for measuring the items of credibility dimensions. Many researchers recommend to use from 5 to 7 categories in this type of scale (e.g. [108]). The reason for using seven or five categories is that it becomes hard for the participants to make such fine distinctions [109]. It is important to note that several source credibility studies employ this kind of scale (e.g. [26]).

Seven social engineering requests have added to the role-play questionnaire to measure susceptibility to social engineering; five of them categories as a high-risk action which involve tricks like the one happen in the real-life on Twitter, for example, Who Viewed My Profile for Twitter and Tvvitterr. The last two requests are categorized as a low-risk action to see their effect of the manipulated variables and examine whether their impact is diverse from the high-risk requests. For example, instead of using a clear fake URL (which viewed as high-risk) like "http://www.Twitterr.com/login/" we provide other URL like "tinyurl.coX/blah". Persuasive messages were associated with every request to help in encouraging the participants to answer and accept those requests as Table II shown. For examining the source who sent the request, the messages wrote in the way make the participants trust on the message source, like these phrases "I try it,,, it really work.", "I recommend you to do it", and so on. In the questionnaire, the participants asked to choose their react on these requests, if the requests sent or tweet by the source (profile owners). To do that, a 5-point Likert scale has been used for every social engineering requests to facilitate measuring the participants' behavior responses on these requests. The rating system for this scale represents as follow "Definitely yes" = 5, "Very probably yes" = 4,

"Probably yes" = 3, "Very probably no" = 2, and "Definitely no" =1 [19].

TABLE II. SOCIAL ENGINEERING REQUESTS/TRICKS AND PERSUASIVE MESSAGES.

Type	Social Engineering Tricks	Persuasive Messages	Risk	Supportive References
Phishing	Through the URL in the message which links the user to a fake Twitter page (phishing website) that informs him to sign-in to his account to proceed.	(via direct message) I'm really surprised,,, Is that you???? tinXurl.com/blah	High	[110]
Phishing	Through message, where the social engineer claiming to be the Twitter Support and they need to confirm the accounts of their users throw pressing this link: http://www.support.twitter.com , while the actual URL displayed in the status bar is: http://www.support.itwitter.com	Your account will be closed in 24h! Confirm it now ,,,, This is important, I lost my old one :(	High	(Twitter Support,2016)
Clickjacking	The tweet present video to trick users into clicking on it, when the user clicks on that video, the attacker will load another malicious page, and the status-message field will be initialized with the URL of that malicious page.	See this video to be able to win with my wonderful prize ,,, don't forget ..retweet it to your friends :)	Low	[111]
Spam or malware	By asking access to the user account before it allows him to watch the video.	I try it ,,, It really interesting ..you can try it ☺.	High	[112]
Clickjacking	The tweet encourages the user to download some documents, while this document contains an executable file as it appears in the link in the statue bar.	You can download the new salary scales in Saudi Arabia ,,, I'm really happy	High	[19]
Downloading	Check who visits your Twitter profile application /software.	Wow, this really works! Finally I found out who visits my profile on Twitter for free!	High	(Who Viewed My Profile for Twitter, 2016) [113]
Clickjacking	Through the link in the message, where the link is written as: https://www.youtube.com/watch?v= 3Um_Hn8, while the actual URL in the status bar is: http://bit.ly/anuyy	(via direct message) I found you in this video you can check it by yourself.	Low	[114]

2) MANIPULATED VARIABLES USING A FRACTIONAL FACTORIAL DESIGN

In many studies, researchers need to perform experiments to define and assess the affected of the factors and to examine the interaction between them. One way to do this is by using an efficient methodology called Fractional Factorial Design. In 1942 Fisher introduce Fractional Factorials for using it in agricultural experiments [115]. Also, Fractional Factorial Designs widely employed in scientific investigations and industrial experiments [116].This design considers as one of the important statistical contributions, use only a fraction of the overall number of possible factor collection under the study. Fractional Factorial design aim to help researchers in reducing the experimental costs by decrease the numbers of experimental runs and saving the participants' efforts [117].

The Full Factorial Design cost a large number of runs because it takes all probable combinations of levels across all such factors. To be more specific, if there are k factors, each at potential levels, Full Factorial Design has 2^k runs. For example, if we want to examine 8 factors in 2-level design; a Full Factorial would result in 2^8 = 256 runs, and this seems to be prohibitively expensive and time-consuming [115]. Sometimes, there aren't adequate resources to use a Full Factorial Design, for that, the researchers attempted to use some subset of all possible runs. The design results from this producer called Fractional Factorials. So, for every k factors across 2 levels, we only run 2^{k-p}. For example, if we have 4 factors, the design will be $2^{4-1}=2^3=8$ runs instead of 16in Full Factorial.[118] address that two-level Fractional Factorial Designs are also known as screening designs because if the experiment has many factors of potential importance, however, only a few that will fall out to be important. Also, he discusses the advantages and disadvantage of these designs. Two-

level Fractional Factorial Designs have many advantages; the first one, as it is previously mention, which is a small number of runs have been used to study a large number of factors. The second one is these designs are orthogonal; means that, every factor's effects are evaluated with extreme precision, which is the same as the precision that would have been acquired if only that factor was under study. Moreover, these designs are also balanced, the same as full factorial designs from which they were derived, for example; factor A is run in the experimental on its various settings in a same number of times. Furthermore, it is a well-chosen design, which is it also have the property that the highest number of potential effects are not confused between each other. While on the other hand, the most important disadvantage of these designs shown when the outcomes of analysis are ambiguous and not clear due to confounding.

On this study, the Fractional Factorial Design will be used to examine the effect of every factor (source characteristic) and the interaction between them. Only 24 Twitter profiles have been resulted from using this design and depending on 14 hypotheses that we want to test it. These profiles were designed to represent 14 Twitter-based source characteristics (the one involve in Hb1 to Hb14) which effect on the user's judgment on the credibility of the attacker to study the effectiveness of them, as shown in Table III. Every experiment contains one profile and in each one, a set of the 14 source characteristics represented by low level (-) or high level (+). Table III presents the design of each experiment and how the characteristics are shown in each profile (experiment) to the participants. For example, the first Twitter profile (experiment 1) have a little interaction in a Twitter domain (have a few number of tweets, multimedia, and favorites), a low number of followers, there is a different interest than the participant, shown his/her real name and picture, and there are common followers between them. In each experiment, we tried to make the remaining of the characteristics that are not belong to it, as average as possible such as the celebrity in experiment 1.

Many challenges are facing this stage, causing of selecting the profiles of the people who represent the characteristics under study and in the same time they well known to the participants. For example, we needed to find a profile of the person who is perceived by the most of the participants as a celebrity, and there is different in the ratio of followers to follows in his profile, on also has a low level of wealth and qualification (experiments 10). Another example is in experiments 17, 18, 19, and 20 where we need to choose Tweets that perceived as in writing, as well as, in choosing characters that have a good or bad appearance. So, to solve these issues, a workshop was performed with a group of participants to select and evaluate all profiles include in each experiment. After that, the selected profiles were added to a role-play experimental questionnaire. It is important to note, that the experiment Fractional Factorial design was performed using Minitab version 17. Minitab is a software package for providing statistical and graphical analysis; it is often used for manipulating the data and for making statistical analysis to sets of data.

3) SCALE DEVELOPMENT AND TESTING

Why we need scaling??? What scale means??? The main reason for doing scaling is to examine a research's hypotheses. A scale is a collection of items around a particular object to understand and measure human emotions, behaviors, attitudes and feelings [119].Scales are developed when researchers want to measures new phenomena that they believe to exist from their theoretical understanding of the world [120]. Develop a good measurement scale is a challenging task that faces many scholars because it will lead to valid and reliable results to their research [121]. There are different types of scales and scaling technique, and the most favorable one is used to suite investigation [122]. Usually, scales are constructed using four types of levels: nominal, ordinal, interval, and ratio. Nominal measurement is used to categories the data with a numeric value (e.g. 1=male; 2=female). The ordinal scale is for ranking data (e.g. student letter grades). Interval level is a combination of nominal and ordinal in which equal intervals between the data have an exact difference between its values (e.g. Temperature in Fahrenheit). The last one is a ratio scale; it is a scale that describes the numerical difference and ratios among the items (e.g. Height, Age). We should note that nominal is the simplest one, while the ratio is the most complicated between them. These levels of scaling are helped in scoring purpose. For that, the researcher can represent the participant responses to a set of items to numbers that explained their attitude or belief. The scaling technique can be categorized to comparative and non-comparative [123]. Comparative scales are used to compare one object with another one. It includes four types of scaling technique which are Pairwise comparison scale, Rank-ordering scale, Constant sum scale and Q-Sort scale. Non-comparative scales are used to evaluate only single object. It includes different types of scaling technique, but here we focus on two types of them which are; Likert scale (it is a measurement scale consists of five responses ranging from strongly disagree to strongly agree, which allow the respondents

to indicate their attitude toward the examined object). The other one is a semantic differential scale (measures people's reactions using a seven-point rating scale toward an antonym pair of words or concepts.). In general, the measurement process begins with generating sample items to evaluate a construct under examination [124].Generating items consider as the most important stage in scale development [125]. In this stage, the researcher should develop a large number of all possible items that demonstrate all aspects of an underlying construct. [120] . Item content can be generated from a various source such as content definition, interviews with the target population and experts in the domain and review of academic literature and relevant articles [126]. So, in this study and for the first three dimensions (Sincerity, Competence, and Attraction) we used the representative items that [19] use it for measure them as shown in Table IV.

TABLE III. THE DESIGN OF THE EXPERIMENTS BASED ON FRACTIONAL FACTORIAL DESIGN.

	Content Interaction	Number of Followers	Common Interests	Having Real Name and Picture	Common Followers	Celebrity	Richness	Qualifications	Ratio of followers to follows	Good Appearance	Good Writing Skills	Message Style	Message Content Interaction	Message Content
Profile/Experiment 1	-1	-1	-1	+1	+1									
Profile/Experiment 2	+1	-1	-1	-1	-1									
Profile/Experiment 3	-1	+1	-1	-1	+1									
Profile/Experiment 4	+1	+1	-1	+1	-1									
Profile/Experiment 5	-1	-1	+1	+1	-1									
Profile/Experiment 6	+1	-1	+1	-1	+1									
Profile/Experiment 7	-1	+1	+1	-1	-1									
Profile/Experiment 8	+1	+1	+1	+1	+1									
Profile/Experiment 9						-1	-1	-1	-1					
Profile/Experiment 10						+1	-1	-1	+1					
Profile/Experiment 11						-1	+1	-1	+1					
Profile/Experiment 12						+1	+1	-1	-1					
Profile/Experiment 13						-1	-1	+1	+1					
Profile/Experiment 14						+1	-1	+1	-1					
Profile/Experiment 15						-1	+1	+1	-1					
Profile/Experiment 16						+1	+1	+1	+1					
Profile/Experiment 17										+1	+1			
Profile/Experiment 18										-1	-1			
Profile/Experiment 19										+1	-1			
Profile/Experiment 20										-1	+1			
Profile/Experiment 21												+1	+1	+1
Profile/Experiment 22												-1	-1	+1
Profile/Experiment 23												+1	-1	-1
Profile/Experiment 24												-1	+1	-1

TABLE IV. MEASUREMENT ITEMS FOR THE FIRST THREE DIMENSIONS.

Sincerity	Competence	Attraction
Honest/ Dishonest	Professional/ Unprofessional	Attractive/ Unattractive
Sincere/ Insincere	Competent/ Incompetent	Expressive/ Inexpressive
Trustworthy/ Not Trustworthy	Qualified/ Unqualified	Appealing/ Unappealing
Safe/ Dangerous	Powerful/ Powerless	Interesting/ Uninteresting
Believable/ Unbelievable	Expert/ Inexpert	Cheerful/ Gloomy
Real-account/ Fake-account	Successful/ Unsuccessful	Exciting/ Dull

While for the last dimension (Reliability), we attempted to search across all studies in the literature that have been using items to measure the credibility (the literature contains studies regarding source credibility in social media, marketing, and online advertising and communication and persuasion). After that, we develop a pool of items (consist of 10 items) that match our dimension (Reliability) as Table VI displayed. Then, we review and select the most suitable six potential items for measuring those dimensions.

To ensure validity, the selected items were reviewed and judge by an information systems scholar to eliminate repetitive and ambiguous items and to make any required changes before we used them. Suggested measurement items for the Reliability dimension are shown in Table VI.

TABLE V: SAMPLE ITEMS BEFORE REFINEMENT FOR RELIABILITY DIMENSION.

Sample Items	Supportive References
Reliable/ Unreliable; Convincing/ Not convincing; Logical / Illogical; Accurate/ Inaccurate; Informative/Not informative; Timely/Untimely; Consistent/Inconsistent; Impressive /Un impressive; Realistic/Unrealistic; Appropriate/Inappropriate.	[32] , [72] , [26] , [23] , [41].

TABLE VI: SUGGESTED MEASUREMENT ITEMS FOR THE RELIABILITY DIMENSION

Dimension	Sample Items	Supportive References
Reliability	Reliable/ Unreliable	[32], [72], [26]], [23], [41]
	Convincing/Not convincing	[26]
	Logical /Illogical	[32], [72].
	Accurate/ Inaccurate	[26], [23], [41]
	Impressive /Unimpressive	[72]
	Realistic/Unrealistic	[32], [26]

	1	2	3	4	5	6	7	
Dishonest	O	O	O	O	O	O	O	Honest
Insincere	O	O	O	O	O	O	O	Sincere
Not Trustworthy	O	O	O	O	O	O	O	Trustworthy
Dangerous	O	O	O	O	O	O	O	Safe
Unbelievable	O	O	O	O	O	O	O	Believable
Fake-account	O	O	O	O	O	O	O	Real-account

Figure 4.1. EXAMPLE OF THE 7- POINT SCALE MEASURE.

4) APPROACH AND PROCEDURES

After we design the experiment and developed a valid measurement scale and test it, we use the validated measurement scale that arises from the pilot study to perform the current experiment. First of all, the SurveyGizmo was used for the experimental questionnaire design and online data collection. SurveyGizmo is an advanced online survey software tool, having more than 40 survey question types, different themes designed, automatic analysis tools and high data security. The survey involves 24 profiles, for every profile we present some information about the profile owner to give a cleared background about his characteristics that we want to examine, which allowed the participants to focus on it. Their corresponding questions contain two parts; the first one is used a 7-point Semantic Differential scale to measure the items of the source credibility dimensions. The second question is for measure the susceptibility to social engineering using 5-point Likert scale, and it consists of two questions one contain low-risk request and the other for a high-risk request. The letter of invitation for this questionnaire was distributed on Twitter in two rounds. The first round distributed by a known male in Twitter and it results in 90 response. Moreover, 110 response resulted from the invitation of the second round which was posts by a famous female in Twitter. In total 200 response was collected for this study. We should note that we offer an award of 1000 Saudi Riyal for one of the participants, to encourage them to participate and give accurate answering. To analysis the collected response, we used SPSS version 24.0 as we will explain in the next chapter.

4. RESEARCH RESULTS

On this stage, we conduct a statistical analysis to convert our data into useful information. This information will help us in determining if the probability of the given research hypothesis is satisfying or not. The process of statistical analysis is done in three steps. First, factor analysis is done for each dimension to extract its properties. After that, we use several statistical analysis techniques to test our hypotheses. So, we start with hypotheses Ha1 to Ha4, then the hypotheses Hb1to Hb2 are discussed.

1) FACTOR ANALYSIS AND DATA SCREENING

Analysis processes for this study start by made factor analysis to test the scale structure and operationalization. The Cronbach's alpha is used to calculate the reliability coefficients for scale items. Then, we found that the reliability of the Cronbach's alpha value for all items under study was 0.96. Moreover, the Cronbach's alpha values for each dimension as follow; Sincerity with six items equal to 0.97, Competence with six items equal to 0.97, Attraction with six items equal to 0.94 and Reliability with six items equal to 0.94. The last one is a susceptibility to social engineering, with two items and the Cronbach's alpha value for it equal to 0.98. The next step is to examine the semantic differential data by using SPSS principal component factor analyses. An eigenvalue of 1 or greater results from factor analysis of the four source credibility dimensions and the susceptibility to social engineering. Table VII display each factor and its item's properties.

2) TESTING HYPOTHESES Ha1 TO Ha4

The results show that there is a positive correlation between every factor of perceived sincerity, competence, attraction, and reliability and the probability of falling as the victim for social engineering as the Pearson correlation coefficient value confirm. The Pearson correlation coefficient value (r) for perceived sincerity equal to 0.54, competence equal to 0.175, attraction equal to 0.42, and reliability equal to 0.52. Most of the correlation coefficients were significant at $p < 0.001$. As we can see that sincerity have the strongest correlation, then reliability, attraction, and the last one is competence. We should note that the R-square equal to 0.29 for sincerity, 0.03 for competence, 0.17 for attraction, and 0.27 for reliability.

3) TESTING HYPOTHESES Hb1 TO Hb14

T-tests have been chosen to examine hypotheses Hb1 to Hb14, to clarify the differences in the responses for the characteristics in each dimension. To do that, we compare all experiment responses that have characteristic under study at low levels with the other one in high levels. So, we start with the first dimension (perceived sincerity) which include hypotheses Hb1 to Hb5. Hypotheses Hb1 to Hb5 suggest that perceive source as sincerity increase, when source's content interaction, source's number of followers, a number of the common followers that the source have with the user increase, and also perceive a source as sincerity is positively related to the sharing common interests with a user and using the real name and picture by the source. Perceived sincerity in the fractional factorial design have eight experiments; four of them contain a characteristic under study in low level, and the other four contains it at a high level. For example, to figure out the impact of the variable "Common Interest", we calculate the responses of the experiments 1, 2, 3, and 4 (for a low level), and then compared it with responses of the experiments 5, 6, 7, and 8 (for a high level). We should note that Cohen's distance (d) also used to clarify the differences of standard deviation between two levels. Table VIII shows the results of both t-tests and effect size of hypotheses Hb1 to Hb14

.

TABLE VII. DIMENSIONS AND ITEM PROPERTIES.

Factor (Dimension) Properties	Items	Number of Observations	Loading	Mean	Standard Deviation	Standard Error
Name: Sincerity Cronbach's alpha: 0.97 Eigenvalue: 5.452 Variance Explained: .25	Honest/Dishonest	200	.967	4.8871	1.04915	.07419
	Sincere/Insincere	200	.960	4.8564	.99764	.07054
	Trustworthy/Not Trustworthy	200	.919	4.9657	1.00590	.07113
	Safe/Dangerous	200	.899	4.5707	1.15956	.08199
	Believable/Unbelievable	200	.816	5.1279	1.05848	.07485
	Real Account/Fake Account	200	.891	4.3507	.95320	.06740
Name: Competence Cronbach's alpha: 0.97 Eigenvalue: 5.554 Variance Explained: .25	Professional/Unprofessional	200	.924	5.3257	.88367	.06249
	Competent/Incompetent	200	.912	5.4443	.91443	.06466
	Qualified/Unqualified	200	.948	5.3293	.88623	.06267
	Powerful/Powerless	200	.938	5.2850	.93018	.06577
	Expert/Inexpert	200	.960	5.3307	.89112	.06301
	Successful/Unsuccessful	200	.872	4.7907	.88711	.06273
Name: Attraction Cronbach's alpha: 0.94 Eigenvalue: 5.605 Variance Explained: .25	Attractive/Unattractive	200	.927	1.8386	.62316	.04406
	Expressive/Inexpressive	200	.893	1.2830	. 90609	.00679
	Appealing/Unappealing	200	.942	1.8779	.62037	.04387
	Interesting/Uninteresting	200	.911	1.9771	.66073	.04672
	Cheerful/Gloomy	200	.972	1.9014	.65620	.04640
	Exciting/Dull	200	.960	1.8664	.68266	.04827
Name: Reliability Cronbach's alpha: 0.94 Eigenvalue: 5.52 Variance Explained: .25	Reliable/ Unreliable	200	.937	2.1551	.70729	.05014
	Convincing/Not convincing	200	.961	2.2541	.65593	.04650
	Logical /Illogical	200	.944	2.3116	.63592	.04508
	Accurate/ Inaccurate	200	.908	2.1342	.68144	.04831
	Impressive / Unimpressive	200	.849	2.2391	.65637	.04653
	Realistic/Unrealistic	200	.921	2.3015	.64398	.04565

Name: Susceptibility to Social Engineering Cronbach's alpha: 0.98 Eigenvalue: 2.79 Variance Explained: 1.72	High request	200	0.73	2.7746	1.33765	.09459
	Low request	200	0.99	2.9015	1.27595	.09022

TABLE VIII. PEARSON CORRELATION COEFFICIENT FOR HYPOTHESES HA1-HA4.

		Susceptibility to Social Engineering	Sincerity	Competence	Attraction	Reliability
Susceptibility to Social Engineering	Pearson Correlation	1	.537**	.175*	.416**	.522**
	Sig. (2-tailed)		.000	.013	.000	.000
	N	200	200	200	200	200
Sincerity	Pearson Correlation	.537**	1	.376**	.556**	.710**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	200	200	200	200	200
Competence	Pearson Correlation	.175*	.376**	1	.360**	.388**
	Sig. (2-tailed)	.013	.000		.000	.000
	N	200	200	200	200	200
Attraction	Pearson Correlation	.416**	.556**	.360**	1	.594**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	200	200	200	200	200
Reliability	Pearson Correlation	.522**	.710**	.388**	.594**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	200	200	200	200	200

** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).

TABLE VII. T-TESTS AND EFFECT SIZES FOR HYPOTHESES HB1-HB14.

Constructs (hypotheses)	Treatment Group	Cases (N)	Standard Deviation	Mean	T Value	P	Mean Difference	Cohen's d
Content Interaction (Hb1)	Low Level	200	0.82	2.84	-30.20	0.01	1.33	4.29
	High Level	200	0.84	4.15				
Number of Followers (Hb2)	Low Level	200	0.91	2.92	-29.09	0.01	1.15	4.13
	High Level	200	0.72	4.07				
Common Interests (Hb3)	Low Level	200	0.69	3.15	-14.18	0.01	0.69	2.01
	High Level	200	0.97	3.84				
Having Real Name and Picture (Hb4)	Low Level	200	0.77	2.90	-29.47	0.01	1.19	4.19
	High Level	200	0.88	4.09				
Common Followers (Hb5)	Low Level	200	0.98	3.36	-4.18	0.01	0.27	0.59
	High Level	200	0.79	3.63				
Celebrity (Hb6)	Low Level	200	0.65	4.10	-7.99	0.01	0.34	1.13
	High Level	200	0.88	4.44				
Richness (Hb7)	Low Level	200	0.78	4.15	-4.08	0.01	0.24	0.58
	High Level	200	0.85	4.39				
Qualifications (Hb8)	Low Level	200	0.73	3.68	-18.95	0.01	1.18	2.69
	High Level	200	0.93	4.86				
Ratio of Followers to Follows (Hb9)	Low Level	200	0.66	4.21	-2.56	0.01	0.12	0.36
	High Level	200	0.89	4.33				
Good Appearance (Hb10)	Low Level	200	1.06	2.81	-8.33	0.01	0.67	1.18
	High Level	200	1.26	3.48				
Good Writing Skills (Hb11)	Low Level	200	1.28	2.79	-8.10	0.01	0.71	1.15
	High Level	200	1.08	3.50				
Message Style (Hb12)	Low Level	200	0.95	3.39	-3.98	0.01	0.27	0.58
	High Level	200	0.74	3.66				
Message Content Interaction (Hb13)	Low Level	200	1.10	3.36	-7.70	0.01	0.45	1.09
	High Level	200	1.19	3.81				
Message Content (Hb14)	Low Level	200	1.11	3.12	-13.85	0.01	0.94	1.97
	High Level	200	1.23	4.06				

There are enough evidences to satisfy hypotheses Hb1 to Hb5 as a following results showed; for content interaction (p-value < 0.01, t value = -30.20, Cohen's d = 4.29),for a number of followers (p-value < 0.01, t value = -29.09, Cohen's d = 4.13),for common interests (p-value < 0.01, t value = -14.18 , Cohen's d = 2.01),for having real name and picture (p-value < 0.01, t value = -29.47, Cohen's d = 4.19), and for common followers (p-value < 0.01, t value = -4.18, Cohen's d = 0.59).T-tests and Cohen's d are also used to test hypotheses Hb6 to Hb14.The results of the t-test show effective influence of celebrity, richness, qualifications and ratio of followers to follows to perceive the source as competent. Similarly, t-test displays significant effects of good appearance and good writing skills that the source has on users' perceptions of attractive. As well as, t-test results present that the message style that the source follows, the content interaction of the source's message and the content of the source's message have a significant impact on perceiving a source as reliable.
The proposed model is beneficial in different ways; first, work as a theoretical foundation for the programmers to develop several applications and tools to help the Twitter users to protect themselves against the social engineering attacks. It also very helpful for the SNS providers to use it in improving the security in the SNS environments.

5. CONCLUSION AND FUTURE WORK

Social networking sites (SNSs), are Internet-based services aim to effective communication between people and share information and knowledge between them. For the past few years, the number of SNSs users

are increasing at an incredible rate, and therefore, its database also becomes huge. Then, from a security perspective, the vulnerability on the SNSs will increase as well. The vulnerability association with social networking sites come through technologies or people. Human factors are seeming to be less study and cover than the technology factors in the research area, even when people consider as the weakest link in security. The most significant risk in the SNSs which is used those vulnerabilities is the social engineering attacks. In social engineering, people are a trick by a social engineer to get critical information or to perform what he wants. The main point that facing social engineering attacks at SNSs is how the SNS users' judgments around the attacker deception requested; this request usually comes in the form of a message. The credibility of attackers is an essential element in users' judgment to obey and refuse social engineering attacks. Therefore, our research is aim to investigate the source credibility dimensions in terms of social engineering, and exploring the characteristics of the source that affect the user's judgment on an attacker as credible, which leads them susceptible to the victimization. All these objectives are examined in the case of Twitter.

For the first objective, the result of this study found that there is a positive correlation between perceiving source as sincerity, competence, attraction, and reliability (source credibility dimensions) and the probability of falling as the victim of social engineering attack. Moreover, perceived sincerity has an ultimate effect on Twitter users' judgment toward accept or reject social engineering requests, then perceived reliability (this dimension have this impact due to the nature of the Twitter and Tweet characteristics) , perceived attraction and last one is perceived competence. This research and [19] agreement on their findings regarding the perceived sincerity (which has the most influence on credibility judgment in the term of social engineering on Facebook). On the other hand, this research and [19] have different finding regarding attraction and competence; Algarni found that the perceived competence have lowest impact on credibility judgment followed by perceived attraction.

For the second objective, the results presented that the source characteristic that has the most significant effect on perceived sincerity is content interaction, then having real name and picture, the number of followers, common interests, and the last one is common followers. In [19], the source characteristics have ordered for this dimension according to its impact as follow; number of friends, the source's use of a real name (this characteristic have the same finding effect to this study), common friends, number of posts, and common beliefs. The source characteristic that has the most significant effect on perceived competence is qualifications, then a celebrity, richness, and finally the ratio of followers to follows. While [19] found the influence on perceived competence as follow; celebrity, qualifications, and wealth (this characteristic have lowest impact like the finding in this study).The source characteristic that has the most significant effect on perceived attraction is good appearance then good writing skills, which are similar to Algarni finding on this dimension. The source characteristic that has the most significant effect on perceived reliability is message content then message content interaction and last one is a message style.

The results of this research have a significant role in several areas. It can help the software developers in understanding the source's (profile) characteristics and used them in building an efficient application that protects the Twitter users against social engineering attacks. Also, the findings can be used to increase the individual's awareness and therefore, prevent and control threats in the organization as a whole. Moreover, this study will help the SNS providers to improve the security of their environment and make it safer for the users. In conclusion, future research can expand to examine another source's characteristics like account age, sexual compatibility and authority in Twitter. Future research could also discuss message credibility to clarify their effect on SNSs users' judgment toward accepting or reject social engineering requests.

Acknowledgments

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

Data Availability

All data is available in the manuscript.

REFERENCES

[1] N. B. Ellison, "Social network sites: Definition, history, and scholarship," Journal of Computer-Mediated Communication, vol. 13, no. 1, pp. 210-230, 2007.

[2] D.-H. Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," Interacting with computers, vol. 22, no. 5, pp. 428-438, 2010.

[3] J. Donath, "Signals in social supernets," Journal of Computer-Mediated Communication, vol. 13, no. 1, pp. 231-251, 2007.

[4] A. Algarni, Y. Xu, C. Taizan, and T. Yu-Chu, "Social engineering in social networking sites: Affect-based model," in Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for, 2013, pp. 508-515.

[5] C. Castillo, M. Mendoza, and B. Poblete, "Information credibility on twitter," in Proceedings of the 20th international conference on World wide web, 2011, pp. 675-684: ACM.

[6] W. Ryan, M. Christopher, H. Jefferson, and M. Jeremy, "The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions," in Social and Human Elements of Information Security: Emerging Trends and Countermeasures, G. Manish and S. Raj, Eds. Hershey, PA, USA: IGI Global, 2009, pp. 43-60.
[7] S. T. Thompson, "Helping the hacker? Library information, security, and social engineering," Information Technology and Libraries, vol. 25, no. 4, p. 222, 2006.
[8] J. Halwar and S. Kadam, "Review on Malicious URL Detection Schemes in Social Networking Site Twitter," 2015.
[9] M. Langheinrich and G. Karjoth, "Social networking and the risk to companies and institutions," Information Security Technical Report, vol. 15, no. 2, pp. 51-56, 2010.
[10] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 71-80: ACM.
[11] A. Al Hasib, "Threats of online social networks," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 11, pp. 288-93, 2009.
[12] N. Marcus, "Why Humans are the Weakest Link," in Social and Human Elements of Information Security: Emerging Trends and Countermeasures, G. Manish and S. Raj, Eds. Hershey, PA, USA: IGI Global, 2009, pp. 15-26.
[13] R. West, C. Mayhorn, J. Hardee, and J. Mendel, "The weakest link: A psychological perspective on why users make poor security decisions," in Social and Human elements of information security: Emerging Trends and countermeasures: IGI Global, 2009, pp. 43-60.
[14] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. J. C. S. J. Richardson, "2005 CSI/FBI computer crime and security survey," vol. 21, no. 3, p. 1, 2005.
[15] A. McIlwraith, Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Gower Publishing, Ltd., 2006.
[16] A. Chitrey, D. Singh, and V. Singh, "A comprehensive study of social engineering based attacks in india to develop a conceptual model," International Journal of Information and Network Security, vol. 1, no. 2, p. 45, 2012.
[17] G. Hogben, "Security issues and recommendations for online social networks," ENISA position paper, vol. 1, pp. 1-36, 2007.
[18] C. I. Hovland, I. L. Janis, and H. H. Kelley, "Communication and persuasion; psychological studies of opinion change," 1953.
[19] A. Algarni, Y. Xu, and T. Chan, "Susceptibility to social engineering in social networking sites: The case of Facebook," 2015.
[20] R. Weber, "Evaluating and developing theories in the information systems discipline," Journal of the Association for Information Systems, vol. 13, no. 1, p. 1, 2012.
[21] S. Gregor, "The nature of theory in information systems," MIS quarterly, pp. 611-642, 2006.
[22] A.-M. Preda, D. A. CRIȘAN, J. L. STĂNICĂ, A. N. A. J. J. o. I. S. SAMUEL, and O. Management, "INNOVATION AND ICT DEVELOPMENT: AN ANALYSIS FOR THE EU-28 MEMBER STATES," vol. 13, no. 2, pp. 154-164, 2019.
[23] R. A. Abdulla, B. Garrison, M. Salwen, P. Driscoll, and D. Casey, "The credibility of newspapers, television news, and online news," in Education in Journalism Annual Convention, Florida USA, 2002.
[24] J. J. Š. p. Žmavc, "Pre-Aristotelian notions of ethos and pathos: the case of Anaximenes' Rhetoric to Alexander," p. 121, 2015.
[25] K. Burke, Language as symbolic action: Essays on life, literature, and method. Univ of California Press, 1966.
[26] M. Eisend, "Source credibility dimensions in marketing communication–A generalized solution," Journal of Empirical Generalizations in Marketing, vol. 10, no. 2, pp. 1-33, 2006.
[27] A. Yaakop, M. M. Anuar, and K. Omar, "Like it or not: Issue of credibility in Facebook advertising," Asian Social Science, vol. 9, no. 3, p. 154, 2013.
[28] R. H. Gass and J. S. Seiter, Persuasion, Social Influence, and Compliance Gaining. Pearson Allyn & Bacon, 2007.
[29] R. H. Gass and J. S. Seiter, Persuasion: Social Influence and Compliance Gaining. Pearson Education, Limited, 2013.
[30] B. Hilligoss and S. Y. Rieh, "Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context," Information Processing & Management, vol. 44, no. 4, pp. 1467-1484, 2008.
[31] R. Ohanian, "Construction and validation of a scale to measure celebrity endorsers' perceived expertise, trustworthiness, and attractiveness," Journal of advertising, vol. 19, no. 3, pp. 39-52, 1990.
[32] D. K. Berlo, J. B. Lemert, and R. J. Mertz, "Dimensions for evaluating the acceptability of message sources," Public opinion quarterly, vol. 33, no. 4, pp. 563-576, 1969.
[33] R. K. Tucker, "On the McCroskey scales for the measurement of ethos," 1971.
[34] J. Mills and J. M. Jellison, "Effect on opinion change of how desirable the communication is to the audience the communicator addressed," Journal of Personality and Social Psychology, vol. 6, no. 1, p. 98, 1967.
[35] R. J. Rhine and L. J. Severance, "Ego-involvement, discrepancy, source credibility, and attitude change," Journal of Personality and Social Psychology, vol. 16, no. 2, p. 175, 1970.
[36] J. Y. Lee and S. S. J. H. C. Sundar, "To tweet or to retweet? That is the question for health professionals on Twitter," vol. 28, no. 5, pp. 509-524, 2013.
[37] S. S. Sundar, "The MAIN model: A heuristic approach to understanding technology effects on credibility," Digital media, youth, and credibility, pp. 73-100, 2008.
[38] S. S. Sundar and C. Nass, "Conceptualizing sources in online news," Journal of Communication, vol. 51, no. 1, pp. 52-72, 2001.
[39] J. B. Walther, "Interpersonal effects in computer-mediated interaction a relational perspective," Communication research, vol. 19, no. 1, pp. 52-90, 1992.
[40] D. Westerman, P. R. Spence, and B. Van Der Heide, "A social network as information: The effect of system generated reports of connectedness on credibility on Twitter," Computers in Human Behavior, vol. 28, no. 1, pp. 199-206, 2012.
[41] M. Kang, "Measuring social media credibility: A study on a Measure of Blog Credibility," Institute for Public Relations, pp. 59-68, 2010.
[42] M. J. Metzger, A. J. Flanagin, K. Eyal, D. R. Lemus, and R. M. McCann, "Credibility for the 21st century: Integrating perspectives on source, message, and media credibility in the contemporary media environment," Communication yearbook, vol. 27, pp. 293-336, 2003.
[43] A. Algarni, Y. Xu, and T. Chan, "Social Engineering in Social Networking Sites: The Art of Impersonation," in Services Computing (SCC), 2014 IEEE International Conference on, 2014, pp. 797-804: IEEE.
[44] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: how good becomes evil," in Proceedings of The 18th Pacific Asia Conference on Information Systems (PACIS 2014), 2014: The Association for Information Systems (AIS).
[45] A. Karami, M. Lundy, F. Webb, and Y. K. J. I. A. Dwivedi, "Twitter and research: a systematic literature review through text mining," vol. 8, pp. 67698-67717, 2020.
[46] D. Westerman, P. R. Spence, and B. Van Der Heide, "Social media as information source: Recency of updates and credibility of information," Journal of Computer-Mediated Communication, vol. 19, no. 2, pp. 171-183, 2014.
[47] H. Kwak, C. Lee, H. Park, and S. Moon, "What is Twitter, a social network or a news media?," in Proceedings of the 19th international conference on World wide web, 2010, pp. 591-600: ACM.
[48] D. Boyd, S. Golder, and G. Lotan, "Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter," in System Sciences (HICSS), 2010 43rd Hawaii International Conference on, 2010, pp. 1-10.
[49] B. Suh, L. Hong, P. Pirolli, and E. H. Chi, "Want to be retweeted? large scale analytics on factors impacting retweet in twitter

network," in Social computing (socialcom), 2010 ieee second international conference on, 2010, pp. 177-184: IEEE.
[50] C. Castillo , M. Mendoza, and B. Poblete Labra, "Predicting information credibility in time-sensitive social media," 2013.
[51] A. Gupta and P. Kumaraguru, "Credibility ranking of tweets during high impact events," in Proceedings of the 1st Workshop on Privacy and Security in Online Social Media, 2012, p. 2: ACM.
[52] Y.-c. Hsu and T. M. J. I. J. o. H.-C. S. Schwen, "The effects of structural cues from multiple metaphors on computer users' information search performance," vol. 58, no. 1, pp. 39-55, 2003.
[53] S. Sikdar, B. Kang, J. O'Donovan, T. Hollerer, and S. Adah, "Understanding information credibility on twitter," in Social Computing (SocialCom), 2013 International Conference on, 2013, pp. 19-24: IEEE.
[54] J. Jiang, Y. Tong, and S. S.-L. Tan, "Do you retweet heath advice on microblogging platforms? The effects of health topic and website design on credibility assessment," 2012.
[55] S. Counts and K. Fisher, "Taking It All In? Visual Attention in Microblog Consumption," ICWSM, vol. 11, pp. 97-104, 2011.
[56] G. M. Armstrong, P. Kotler, M. Harker, and R. Brennan, Marketing: an introduction. Pearson UK, 2018.
[57] F. J. Riggins and H.-S. J. C. o. t. A. Rhee, "Toward a unified view of electronic commerce," vol. 41, no. 10, pp. 88-95, 1998.
[58] E. Bayer, S. Srinivasan, E. J. Riedl, and B. J. I. J. o. R. i. M. Skiera, "The impact of online display advertising and paid search advertising relative to offline advertising on firm performance and firm value," 2020.
[59] Z. J. J. P. Reich, "Source credibility and journalism: Between visceral and discretional judgment," vol. 5, no. 1, pp. 51-67, 2011.
[60] S. B. MacKenzie and R. J. Lutz, "An empirical examination of the structural antecedents of attitude toward the ad in an advertising pretesting context," The Journal of Marketing, pp. 48-65, 1989.
[61] M. J. Metzger and A. J. J. J. o. p. Flanagin, "Credibility and trust of information in online environments: The use of cognitive heuristics," vol. 59, pp. 210-220, 2013.
[62] M. J. Metzger, A. J. Flanagin, K. Eyal, D. R. Lemus, and R. M. J. A. o. t. I. C. A. McCann, "Credibility for the 21st century: Integrating perspectives on source, message, and media credibility in the contemporary media environment," vol. 27, no. 1, pp. 293-335, 2003.
[63] X. Nan, "Perceived source credibility and advertising persuasiveness: An investigation of moderators and psychological processes," Journal of Current Issues & Research in Advertising, vol. 34, no. 2, pp. 195-211, 2013.
[64] J. D. Greer, "Evaluating the credibility of online information: A test of source and advertising influence," Mass Communication and Society, vol. 6, no. 1, pp. 11-28, 2003.
[65] A. Verma et al., "2014 focused update of the Canadian Cardiovascular Society Guidelines for the management of atrial fibrillation," vol. 30, no. 10, pp. 1114-1130, 2014.
[66] J. J. J. o. P. B. A. McGuire and M. Physics, "Non-orthogonality in the strong potential Born approximation," vol. 18, no. 3, p. L75, 1985.
[67] B. A. Lafferty and R. E. J. J. o. b. r. Goldsmith, "Corporate credibility's role in consumers' attitudes and purchase intentions when a high versus a low credibility endorser is used in the ad," vol. 44, no. 2, pp. 109-116, 1999.
[68] S. Kim, S. M. J. I. J. o. I. M. Choi, and Advertising, "Credibility cues in online shopping: an examination of corporate credibility, retailer reputation, and product review credibility," vol. 7, no. 3, pp. 217-236, 2012.
[69] A. J. I. P. Gralewska-Vickery and Management, "Communication and information needs of earth science engineers," vol. 12, no. 4, pp. 251-282, 1976.
[70] S. R. Murray and J. J. J. o. M. I. Peyrefitte, "Knowledge type and communication media choice in the knowledge transfer process," pp. 111-133, 2007.
[71] P. Kearney, T. G. Plax, V. P. Richmond, and J. C. McCroskey, "Power in the classroom III: Teacher communication techniques and messages," Communication Education, vol. 34, no. 1, pp. 19-28, 1985.
[72] J. C. McCroskey, W. Holdridge, and J. K. Toomb, "An instrument for measuring the source credibility of basic speech communication instructors," Communication Education, vol. 23, no. 1, pp. 26-33, 1974.
[73] M. A. Hewgill and G. R. Miller, "Source credibility and response to fear-arousing communications," 1965.
[74] T.-H. J. T. J. o. s. p. Choo, "Communicator credibility and communication discrepancy as determinants of opinion change," vol. 64, no. 1, pp. 65-76, 1964.
[75] H. W. Simons, "Persuasion," Reading, Mass, 1976.
[76] E. McGinnies, "Initial attitude, source credibility, and involvement as factors in persuasion," Journal of Experimental Social Psychology, vol. 9, no. 4, pp. 285-296, 1973.
[77] E. McGinnies and C. D. Ward, "Better liked than right trustworthiness and expertise as factors in credibility," Personality and Social Psychology Bulletin, vol. 6, no. 3, pp. 467-472, 1980.
[78] C. I. Hovland and W. Weiss, "The influence of source credibility on communication effectiveness," Public opinion quarterly, vol. 15, no. 4, pp. 635-650, 1951.
[79] S. P. Jain and S. S. Posavac, "Pre-purchase attribute verifiability, source credibility, and persuasion," 1999.
[80] B. S. Greenberg and P. H. Tannenbaum, "The effects of bylines on attitude change," Journalism & Mass Communication Quarterly, vol. 38, no. 4, pp. 535-537, 1961.
[81] J. Mills and J. Harvey, "Opinion change as a function of when information about the communicator is received and whether he is attractive or expert," Journal of Personality and Social Psychology, vol. 21, no. 1, p. 52, 1972.
[82] C. D. Ward and E. McGinnies, "Persuasive effects of early and late mention of credible and noncredible sources," The Journal of Psychology, vol. 86, no. 1, pp. 17-23, 1974.
[83] D. M. Wegner, R. Wenzlaff, R. M. Kerker, and A. E. Beattie, "Incrimination through innuendo: Can media questions become public answers?," Journal of Personality and Social Psychology, vol. 40, no. 5, p. 822, 1981.
[84] A. Bhattacherjee and N. Hikmet, "Physicians' resistance toward healthcare information technology: a theoretical model and empirical test," European Journal of Information Systems, vol. 16, no. 6, pp. 725-737, 2007.
[85] L. W. Jones, R. C. Sinclair, and K. S. Courneya, "The effects of source credibility and message framing on exercise intentions, behaviors, and attitudes: an integration of the elaboration likelihood model and prospect theory1," Journal of Applied Social Psychology, vol. 33, no. 1, pp. 179-196, 2003.
[86] R. E. Petty and J. T. Cacioppo, The elaboration likelihood model of persuasion. Springer, 1986.
[87] S. Chaiken and D. Maheswaran, "Heuristic processing can bias systematic processing: effects of source credibility, argument ambiguity, and task importance on attitude judgment," Journal of personality and social psychology, vol. 66, no. 3, p. 460, 1994.
[88] J. Long, No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress, 2011.
[89] J. Nagy and P. Pecho, "Social networks security," in 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 321-325: IEEE.
[90] P. Kaul and D. J. I. J. o. C. A. Sharma, "Study of automated social engineering, its vulnerabilities, threats and suggested countermeasures," vol. 67, no. 7, pp. 13-16, 2013.
[91] Z. M. Aljazzaf, M. Perry, and M. A. Capretz, "Online trust: Definition and principles," in Computing in the Global Information Technology (ICCGI), 2010 Fifth International Multi-Conference on, 2010, pp. 163-168: IEEE.
[92] T. Qin and J. K. Burgoon, "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering," in Intelligence and Security Informatics, 2007 IEEE, 2007, pp. 152-159.

[93] W. H. Tolman, Social engineering: A record of things done by American industrialists employing upwards of one and one-half million of people. McGraw Publishing Company, 1909.
[94] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Toward understanding social engineering," in The Proceedings of the 8th International Conference on Legal, Security and Privacy Issues in IT Law,(Critical Analysis and Legal Reasoning), 2013, pp. 279-300: The International Association of IT Lawyers (IAITL).
[95] A. W. J. S. P. Wood and Policy, "Exploitation," vol. 12, no. 2, pp. 136-158, 1995.
[96] J. J. C. f. d. Servaes and s. change, "Communication for development approaches of some governmental and non-governmental agencies," p. 201, 2008.
[97] A. Singhal and E. M. Rogers, "A theoretical agenda for entertainment—education," Communication theory, vol. 12, no. 2, pp. 117-135, 2002.
[98] E. Moyer-Gusé, "Toward a theory of entertainment persuasion: Explaining the persuasive effects of entertainment-education messages," Communication Theory, vol. 18, no. 3, pp. 407-425, 2008.
[99] S. T. Murphy, L. B. Frank, M. B. Moran, and P. Patnoe-Woodley, "Involved, transported, or emotional? Exploring the determinants of change in knowledge, attitudes, and behavior in entertainment-education," Journal of Communication, vol. 61, no. 3, pp. 407-431, 2011.
[100] D. Craciun, "Role–playing as a creative method in science education," Journal of Science and Arts, vol. 1, no. 12, pp. 175-182, 2010.
[101] C. Sleigh, "Using Role Play as a Way in to the History of Science," Learning and Teaching in Philosophical and Religious Studies, p. 131, 2004.
[102] A. Maley, "Role play," ed: Resource books for teachers, 1987.
[103] G. A. Fine, Shared fantasy: Role playing games as social worlds. University of Chicago Press, 2002.
[104] K. M. Yardley-Matwiejczuk, Role Play: Theory and Practice. Sage Publications (CA), 1997.
[105] M. Lewis-Beck, A. E. Bryman, and T. F. Liao, The Sage encyclopedia of social science research methods. Sage Publications, 2003.
[106] J. S. Downs, M. Holbrook, and L. F. Cranor, "Behavioral response to phishing risk," in Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, 2007, pp. 37-44: ACM.
[107] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010, pp. 373-382: ACM.
[108] R. Garland, "A comparison of three forms of the semantic differential," Marketing Bulletin, vol. 1, no. 1, pp. 19-24, 1990.
[109] M. Danial, "Doing quantitative research in education," ed: Sage Publication, London, 2004.
[110] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, "PhishAri: Automatic realtime phishing detection on twitter," in eCrime Researchers Summit (eCrime), 2012, 2012, pp. 1-12: IEEE.
[111] M. Balduzzi, M. Egele, E. Kirda, D. Balzarotti, and C. Kruegel, "A solution for the automated detection of clickjacking attacks," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 135-144: ACM.
[112] A. Sanzgiri, J. Joyce, and S. Upadhyaya, "The early (tweet-ing) bird spreads the worm: An assessment of twitter for malware propagation," Procedia Computer Science, vol. 10, pp. 705-712, 2012.
[113] A. Sadeghian, M. Zamani, and B. Shanmugam, "Security threats in online social networks," in Informatics and Creative Multimedia (ICICM), 2013 International Conference on, 2013, pp. 254-258: IEEE.
[114] H. Shahriar and H. Haddad, "Security assessment of clickjacking risks in web applications: metrics based approach," in Proceedings of the 30th Annual ACM Symposium on Applied Computing, 2015, pp. 791-797: ACM.
[115] F. P. Stewart, "Fractional Factorial Designs," Encyclopedia of Biostatistics, 2005.
[116] K. Hinkelmann and O. Kempthorne, Design and Analysis of Experiments, Special Designs and Applications. Wiley, 2012.
[117] R. F. Gunst and R. L. Mason, "Fractional factorial design," Wiley Interdisciplinary Reviews: Computational Statistics, vol. 1, no. 2, pp. 234-244, 2009.
[118] J. G. Voelkel, "Fractional Factorial Designs," Encyclopedia of Statistics in Quality and Reliability, 2007.
[119] C. A. Mahoney, D. L. Thombs, and C. Z. Howe, "The art and science of scale development in health education research," Health Education Research, vol. 10, no. 1, pp. 1-10, 1995.
[120] R. F. DeVellis, Scale development: Theory and applications. Sage publications, 2012.
[121] A. Slavec and M. Drnovsek, "A perspective on scale development in entrepreneurship research," Economic and Business Review for Central and South-Eastern Europe, vol. 14, no. 1, p. 39, 2012.
[122] J. A. Khan, Research Methodology. APH Publishing Corporation, 2011.
[123] D. C. N. Sodhi, Research Methodology: Concepts and Cases. 2011.
[124] T. R. Hinkin, J. B. Tracey, and C. A. Enz, "Scale construction: Developing reliable and valid measurement instruments," Journal of Hospitality & Tourism Research, vol. 21, no. 1, pp. 100-120, 1997.
[125] T. R. Hinkin, "A review of scale development practices in the study of organizations," Journal of management, vol. 21, no. 5, pp. 967-988, 1995.
[126] A. Selbo-Bruns, F. J. Floyd, and S. N. Haynes, "Scale Development," The Encyclopedia of Clinical Psychology, 2015.