Inattentional Blindness Factors that Make People Vulnerable to Security Threats in Social Networking Sites

Abdullah Algarni*
Information Technology Division, Institute of Public Administration, Riyadh, Saudi Arabia.

* Corresponding author. Email: algarniaa@ipa.edu.sa
Manuscript submitted January 10, 2019; accepted March 15, 2019.
doi: 10.17706/jcp.14.3.184-194

Abstract: Over the past decade, Social Networking Sites (SNSs) have been providing benefits and opportunities for millions of users. However, attackers and deceptive users have been trying to take advantage of SNSs popularity and launch many types of attacks such as phishing, click-jacking, spamming, malware, or providing misleading and false information. Past research showed that SNSs users are more vulnerable to many security attacks than any other media such as email, electronic newspaper or any other online environment. Yet little research has empirically explored the characteristics of the virtual environments of SNSs, which make users such vulnerable. Using ethnography method, existing study has pointed eight factors that influence inattentional blindness of SNSs users, and therefore make them vulnerable to security threats in SNSs.

Key words: Information security, cybersecurity, social networking sites, social media, inattentional blindness, perceptual blindness.

1. Introduction

Social Networking Sites (SNSs) have spread rapidly over the past decade. SNSs is now part of everyday life for the majority of people in world. SNSs have provided new ways of connections between people, professionals, and organizations. In addition, SNSs have provided new ways of socially driven information discovery. Although SNSs offer tremendous opportunities, growth of SNSs raises new security risks and growing concerns in regards to identity, privacy, and deception. In addition, SNSs include groups of people who have never met in person but communicate with each other through SNSs to share knowledge, opinions, interests and activities. Unfortunately, large percentage of information posted on SNSs is not trusted, and in many cases, is not safe.

Past research showed that SNSs users are more vulnerable to many security attacks than the users of any other online environment such as email, electronic newspaper or any other normal webpages (e.g., [1]-[8]). Previous research on SNSs users' vulnerabilities has focused on the characteristics of users that make them more vulnerable to security attacks, such as personality traits, demographics, or their online habits in SNSs (e.g., [9]-[13]). Yet little research has empirically explored the characteristics of the virtual environments of SNSs that influence the inattentional blindness (or perceptual blindness) of the users, which make them such vulnerable to security threats in SNSs. This study has explored eight factors that influence inattentional blindness of SNSs. These factors make people more vulnerable to security threats in SNSs than

any other online environment.

2. Literature Review

SNSs includes many types of contents such as news, stories, blogs, tags, posts, notes, videos, photos, and hyperlinks. Facebook users, for example, share more than 30 billion pieces of content each month [14]. There are several studies that have investigated and highlighted the security threats in SNSs (e.g., [1]-[4], [15]-[17]). Unsecure practices used when dealing with content available on SNSs leads people to fall victim to many security threats. The content may have malicious software such as viruses and worms. This content can be embedded in posts or messages through a hyperlink that leads to an executable file, or to a hyperlink on a page that includes another hyperlink to an executable file with some instructions that trick the victim into downloading that file [16].

Phishing is also a potential threat in SNSs. Phishing can be posted in SNSs as stories, offers, or alert messages that attract victims to download an attachment or click on an embedded hyperlink [18]. Spam is another example of such threats, and it is a critical issue since research suggests that SNSs may replace e-mail as a means of communication [16]. For those SNSs that allow users to post HTML in their profiles, users are vulnerable to cross-site scripting attacks (XSS), which enable attackers to install client-side scripts into a profile that is viewed by other users [16]. In addition, "defamation" and "ballot stuffing" can be used, which are attacks that aim to destroy the reputation of a person or system [19].

People, in general, think that they are good at detecting deception and lies. However, research indicates that people have weakness and therefore perform poorly in detecting deception [20], [21]. The strong relationship between deception and perception illustrates the complexity of detecting and controlling security threats in SNSs. On the organizational level, the findings of a study done by [22] suggest that attackers could succeed even among those organizations that identify themselves as being aware of security threats.

Marett, Biros, and Knode (2004) have explained that the reason why people are weak and perform poorly in detecting deception is because of the "lie detector bias," which is the assumption that most people are telling the truth [23]. Most of the books and studies that have been published indicate that the main cause of human weaknesses in terms of information security is human socio-psychological characteristics [18], [24]-[26]. There are some works that have discussed the psychology of human vulnerability explicitly to understand why humans are the weakest link in information security, such as [24], [27]-[30]. However, their discussions are based on what have been published in different areas of studies such as persuasion and influence in marketing, especially the principles of influence by Cialdini [31]. The main limitation of those works is that the nature and the purpose of persuasion and influence in marketing are different than security threats in SNSs.

West, Mayhorn, Hardee, and Mendel (2009) divided the psychological perspective of why users make poor security decisions to three sections: (1) User factors, such as problem solving limitation and decision making heuristic and experience; (2) technology factors, such as the credible appearance and personal relevance of the e-mail or website that tricks the users; and (3) environmental factors, such as inattentional blindness, where users may not perceive details of the threat [32]. Inattentional blindness is a psychological lack of attention that makes individual fails to perceive an unexpected stimulus that is in plain sight [33], [34]. This study aims to address the third type (environmental factors) by exploring the environmental-based factors that increase the inattentional blindness of the users, and therefore increase their vulnerability to security threats.

3. Method

3.1. Using Qualitative Method

Qualitative research is the research method that is used to gain a deep understanding of the human behavior as well as the different reasons that govern such behavior that the individuals have. The qualitative method usually engages in the investigations with regards to the how and the why of the decision making rather than just focus on the when, where and the what thus they usually make use of small sample as opposed to large or very large samples. The qualitative method usually produces information with regards to particular cases that are being explored [35].

There are a number of data collection methods that are always applied in the qualitative research method. First, there is the focus group which is used to elicit information concerning the different cultural norms of the different groups as well as the generation of broad viewpoints about different issues of concern to the subgroups or the cultural groups that are being explored in the study [36]. Secondly, there are in-depth interviews which are important for the collection of data with regards to the personal histories of the different individuals, the experiences and the perspectives of the people especially with regards to a number of sensitive issues [37]. Also, there is the use of participant observation where the naturally occurring behaviors of the different individuals are considered in their natural contexts.

On the other hand, there are number of approaches that can be used in qualitative research. The most common approaches that can be used in qualitative research are narrative, phenomenology, grounded theory, ethnography, and case study.

3.2. Using Ethnography

The main purpose of the present study is to explore the inattentional blindness factors that make people vulnerable to security threats in SNSs. To achieve this aim, ethnography approach has been used. Ethnographic research is a broad school, lacking a single or uncontested definition. However, there is an agreement between researchers that the ethnographic method mainly focuses on people in their lived environment. Ethnographic method is about exploring and understanding people in their day-to-day environment. Key ethnographic theorists agree on the methods required to achieve this end. First, participant observations are commonly used in ethnography. Participant observations involve the detached observation of people's behaviours, mannerisms, interactions and relationships. In fact, ethnographic researchers use participant observations to observe all facets of people's day-to-day lives.

Second, in depth interviews are also commonly used in ethnography. That is, qualitative interviews are recognised as an ethnographic methods separate to participant observations. While in depth interviews are frequently used in behaviour research alone, they are usually used along with observations in ethnography, to further understand the meanings and perspectives of the observed behaviours [38]. As such, in depth interviews are often conducted during phases of participant observations; with interviewing predominately taking an unstructured form [38].

When doing ethnography, researcher listens to the conversations of the participants, read the documents produced by the organization under study, and ask people questions. Yet what most distinguishes ethnography from other methodologies is a more active role assigned to the cognitive modes of observing, watching, seeing, and discussing. In this study, the application of ethnography included the following procedures:

1. Establishing a direct relationship with participants.
2. Following and browsing participants SNSs accounts.
3. Observing and describing participants' social actions.
4. Interacting with participants and participating in their everyday ceremonials and rituals.

5. Learning as much as we can of the participants' code in order to understand the meaning of their actions.

The goal of the previous procedures is to understand participants' perceptions, attitudes and behaviors in regard to dealing with security threats. Participants' profiles and timelines in SNSs save and keep a record of individuals' activities on their accounts and their interactions when dealing with others, such as sharing, posting, liking and commenting. The profiles and timelines also show the groups, events, friends and commercial pages that the users are members of. The observation and interviews have been used in many areas of behavioral research, such as psychology, sociology, nursing and information systems. The observation and interviews methods can be structured, unstructured or a mix of both structured and unstructured (e.g.,[39]-[41]). As the observations and interviews in the present study commenced without predetermined notions, they were mostly unstructured. In this study, 27 participants have been used. Data have been collected during 2017, using both observations and interviews at the same time.

3.3. Sample and Participants

Theoretical sampling technique [42] was adopted while choosing the participants. In theoretical sampling, researcher chooses the participants selectively and theoretically, in which it helps the researcher best form the theory [42], [43]. Literature indicates (e.g., [43]) that people behaviours in SNSs are affected by their risk perception, awareness level, and demographic variables, such as age, gender, and educational level. Therefore, we selected a sample that represents a potentially high degree of variation in their experiences and demographics in order to explore all possible factors. Table 1 shows the 27 participants that have participated in this study.

Table 1. Sample

Variable	N (=27)	Percentage
Nationality		
Saudis	15	55%
Egyptians	7	26%
Americans	5	19%
Gender		
Male	16	59%
Female	11	41%
Age		
From 18-25	7	26%
From 26-35	8	27%
From 36-45	5	19%
Over 45 years old	7	26%
Education level		
Lower than a bachelor's	7	26%
Bachelor's	9	33%
Master's	7	26%
PhD	4	15%
Time elapsed since joining SNSs		
Less than 6 months	3	11%
6 month - less than 1 year	5	19%
1 year – less than 2 years	7	26%
2 years or more	12	44%
Education background		
IT related	9	33%
Not IT related	18	67%

3.4. Analysis

This study used content analysis, in which codes and themes are derived inductively from the interview transcripts and observations' notes. Content analysis is widely used in ethnographic studies [36]. This analysis technique supports the qualitative description through a reporting of meanings, reality, and experiences. Manual data analysis started after the observation and the interview with the first participant, and conducted concurrently with data collection. As suggested by [36], Initial codes were generated by labelling data extracts with a code reflecting the meaning of the extract. These codes were then collated into potential themes. This coding was followed by an iterative process, in which the themes were reviewed with the coded extracts and the entire dataset. This review was conducted to ensure the consistent application of codes and themes, and to generate a thematic map of the analysis and clear definitions and names for each theme.

4. Result

The analysis and coding of the collected data revealed some factors that influence inattentional blindness of SNSs users, and therefore make them vulnerable to security threats. The resulted factors are explained in the following sections.

4.1. It's Free since There is no Money Charge

The collected data showed that most participants do not realize the value of information, and consider the price as if it is money only. For example, Participant 9 reported:

As long as no charge, I don't bother myself with hiding information

This factor can be abused by deceptive attackers to gain more information from potential victims. That is, they provide any service or product and assume that it's for free! However, in order to get those services or product, the victim has to provide some information such as name, email address, zip code, or telephone number. This trick is also seen in watching video, play game, download or use an application, browsing or downloading a book and so on.

4.2. I'm Safe since I'm Anonymous

The observations and the interviews revealed that participants how use nicknames in SNSs think that they are safer and more secured when they are anonymous. For instance, Participant 3 said:

My profile is nicknamed, and I had that mentality in life – the more people know about you, the more vulnerable you are.

The observation revealed that anonymous users do not control their behaviours as much as they do when they are identifiable. By comparing the behaviour of the users who use their real names and the users who use nicknames, we found that anonymous users perceive threats as less harmful to them, and perceive themselves as less susceptible to the threats than those who use their real names. This belief makes the users who use nicknames more impulsive to subscribe to more untrusted pages or groups, more impulsive to accept friendship invitations from strangers, more impulsive to make conversations with strangers, and more impulsive to reveal private information about their own life or about their works.

I have two accounts. One account has a real name while the other has a nickname. The real account is the one I use carefully most of the time and it is for my career endeavors, family and friends' purposes. The account that I use nicknames is meant for doing staff that require no restrictions. (Participant 7)

4.3. I Don't Know How did I Get This

The observations of the participants showed another important factor that makes SNSs a distinguish online environment. That is, we found that SNSs users see, read, or watch what others choose to show them, not what they choose to see, read, or watch. Some SNSs have some filters that allow the users to choose who can see their posts, videos, or stories, in which they can select specific group of users and post that content to them. However, most of SNSs do not have a feature that allows the users to filter the contents that appear to them. In regards to this point, Participant 23 cited:

> *I don't like politics but as you can see my friends keep posting about the conflict between USA and Rusha. I wish there is a filter in Facebook or Twitter that allows me to weed out those posts that don't match my interest.*

As such, SNSs users don't have a control on which contents that appeared in their profiles or accounts. This allows attackers to reach a large number of victims and broadcast their tricks to many users in easy way. As long as the attacker has a friendship connection with someone, or subscribe to a page or a group, the attacker can distribute it to that connected users, and those users will run across any tricks the attacker make. This factor can be worse when the user subscribes to an open page or group where attackers can join and post their tricks. The observations revealed that Participant 11 uses a suspicious application that posts automatically on his behave. When we asked him about this application he said:

> *This application is recommended to me by a member of an open group on Facebook… I don't know that specific user offline but I'm a member of that group since a couple of months.*

4.4. I Don't Know Why I'm Reading This

The observation of the participants showed that SNSs read and watch almost every content. The participants during interviews also indicate that they read and watch every content. When one of the participants asked about the reason behind this, he answered:

> *Yes, I scan almost every content that appears on my account simply because most SNSs don't have different sections that categorize topics or news. As soon as a user posts or wrote something, it appears on my account and therefore I will go through it.*

This is different than the case in newspaper, books, and other websites, where people search for a specific topic to read or a specific video to watch. Some participants cited that they read most of the contents because those contents are short and don't require a long time like the case of reading a book or newspaper. Other participants justify this by saying that those contents as recommended by their friends, and therefore that content should be of interest.

4.5. I Trust Him Because He Always Likes My Posts

The collected data revealed that all participants love compliment, appreciation and nice words, and they like, trust, and become more vulnerable to those who compliment them. All participants indicate (in a direct or in an indirect way) that they get happy and excited when other users compliment or say nice words about them, their posts, or their photos. Most of them indicate that the most interesting thing they want to know when they login to their accounts is how many users press "like" under their participations or contents, or if any user has written any nice words about them.

Moreover, most of the participants say that the trust that has been built between them and strangers is based on continues compliment, pressing "Like", and nice words that they have received from those

strangers. This factor affects not only users who use their real names, but anonymous users also love compliment, appreciation and nice words. They also trust and feel attracted to those strangers who compliment, appreciate, or say nice words about them or their contents.

Although we have never met, I found his interactions with my posts and photos as an excuse to trust him and care about him.

This trick can be abused by attackers to gain victims' trust. If certain trust has been made, victims are more likely will reveal some critical information or perform some actions that attackers request.

4.6. I Made It for Him Because He Made it for Me First

The interviews with participants showed another important factor related to reciprocity. That is, we fount that participants are more willing to perform an action to someone did the same first. Some participants indicate that they feel guilty to refuse an order from someone did the same thing first. They say that when someone introduces his/her name to them in a conversation for example, they immediately reveal their names. Also, when someone talks about his location, work, family, or other information, they also do the same. This trick can be abused by attackers in order to gain the victims' trust, and therefore influence them to perform an action or to reveal an information that benefits that attacker.

In fact, the influence of reciprocity has been mentioned repeatedly in the literature. Many researchers (e.g., [28], [31], [44], [45]) suggest that when people receive presents or assistance from other people, in as much as they may be free, they develop a feeling of discordance until favors are reciprocated. A person will have a penchant to give back in an equal measure whenever a chance presents itself. This factor has been also observed clearly in this study.

4.7. I Thought SNSs Providers will Take Care of This

The interviews with participants showed that they rely heavily on SNSs providers. We found that participants trust SNSs providers and think that those providers will ensure the security and protect the privacy of the users.

I think Facebook, Twitter, or Snapchat have their own security forces, and will do this job for me. (Participant 3)

Another example is reported by Participant 21, when she asked about some games that she play frequently in SNSs, and whether she know if this game is secured and trustworthy or not, she answered by saying:

Since SNSs providers allowed those games to be run on SNSs that means that they are safe.

Similar opinions have been collected also from the participants regarding applications, videos, advertisements, and other contents. Unfortunately, SNSs providers can not control all threats in SNSs. In addition, the priority of the majority of SNS providers is profit, which can be achieved by attracting as many users as possible, and attracting more companies that advertise on their sites. This goal, however, sometimes contradicts the security of individuals. This can be observed in the case of creating a new account in Facebook, which requires only an email address for authentication. This allows attackers to create as many profiles, pagers, or event as they want, including profiles with fake and impersonated identities.

4.8. I Do This Because Many SNSs Users Do it

The interviews with participants showed a strong effect of social influence in SNSs. The collected data revealed that most of participants do what other users do regardless of the importance or the safety of that action. In addition, majority of participants assume that the behaviours and the actions of other SNSs users are correct behaviour. The number of users who do certain action positively affects how other users perceive such action. For example, participant 23 when she asked about a game she downloaded,

I would consider the number of users who downloaded the game as cues to make judgment about it.

Moreover, followers, fans, views, likes, favorites, and comments that a user has made, also positively affects how other users perceive that user.

No, I don't think this is a fake profile, see how many followers he has

In fact, social influence (also called social proof) has been discussed in literature, and it has been found to be one of the more powerful strategies in persuasion [46]. The risk of this principle from the security perspective is that SNSs users behave according to the general attitude rather than what is secure.
By comparing SNSs and other online environments such as newspaper or email, we can see that the users of newspaper or email don't observe most of other users' behaviours, while in SNSs the users observe each other behaviours. This fact increases the risk of social influence in SNSs.

5. Discussion and Conclusion

The findings of this study make a significant contribution, directly or indirectly, to the literature in several areas of study such as perception, deception, persuasion and information security management. Several studies in information systems have investigated individuals' venerability to security victimisation by relying on a number of theories and techniques, such as protection motivation theory (e.g., [47]-[49]), electroencephalography (e.g., [50]), technology threat avoidance theory [51], and routine activity theory (e.g., [52]). There seems to be a general agreement that an individual's compliance with attackers' deceptions is associated with making accurate judgments regarding threat. This study contributes to this stream of research by explaining the impact of the inattentional blindness factors associated with SNSs environment, on individuals' compliance behaviours.

Understanding the attitudes, cognition and behavioural intentions of individuals in response to threat is a key element in information security. An application of protection motivation theory in the information security context [48] found that coping appraisal factors such as response efficacy, risk perception, self efficacy and response costs, play a vital role in individuals' behaviours regarding security threats, for both ordinary organisational employees and information security professionals. People's response efficacy, risk perception, self-efficacy and response costs are associated with making accurate judgments regarding risk. The factors that have been found in this study explained some of SNSs environmental factors that reduce users' risk perception, and that reduce users' ability to make accurate judgments regarding risk. Through the inattentional blindness factors (perceptual blindness) associated with SNSs that have been explored in this study, and through the creation of a misleading perception (illusion), the attacker makes the victim in SNSs feel safe and therefore not able to perceive the threat.

This study makes also a significant contribution to the industry by attempting to understand and solve a serious problem in information security. The context of the study reflects another significance dimension of the contribution. SNSs are a common source of security threats nowadays [1]-[4], [16]. SNS users have been found to be very vulnerable to falling victim to many security attacks such as phishing, clickjacking, sexual

abuse, financial abuse, identity theft, impersonation, physical crime, and many other forms of attack. This means that this study addresses a crucial problem in information security for both individuals and organizations.

Finally, while this study makes a significant contribution to both literature and industry, there are two main limitations worth noting. First, this study used a qualitative method, and the main limitation of any qualitative method is the subjective interpretation bias. Bias can occur in qualitative studies where a researcher has to interpret the data to explore the most important factors under study. The second general limitation is that qualitative methods cannot determine the existence of a relationship between the factors under study and users' demographics due to the small number of participants. However, these limitations are common in qualitative studies and future research can utilise other creative methodologies to avoid the limitations of this study.

References

[1] Nagy, J., & Pecho, P. (2009). *Social Networks Security,* 321-325.

[2] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50(10),* 94-100.

[3] Dimensional-Research. (2011). The risk of social engineering on information security: A survey of it professionals. *Book The Risk of Social Engineering on Information Security: A Survey of It Professionals*.

[4] Chitrey, A., Singh, D., & Singh, V. (2012). A comprehensive study of social engineering based attacks in India to develop a conceptual model. *International Journal of Information and Network Security (IJINS), 1(2),* pp. 45-53.

[5] Algarni, A., Xu, Y., Chan, T., & Tian, Y. C. (2013). Social engineering in social networking sites: Affect-based model. In Editor (Ed.), *Book Social Engineering in Social Networking Sites: Affect-Based Model* (pp. 508-515).

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

[7] Braun, R., & Esswein, W. (2013). Towards a conceptualization of corporate risks in online social networks: A literature based overview of risks. In *Book Towards a Conceptualization of Corporate Risks in Online Social Networks: A Literature Based Overview of Risks* (pp. 267-274).

[8] Algarni, A., & Xu, Y. (2013). Social engineering in social networking sites: Phase-based and source-based models. *International Journal of e-Education, e-Business, e-Management and e-Learning, 3(6),* 456-462.

[9] Algarni, A., Xu, Y., & Chan, T. (2014). Social engineering in social networking sites: The art of impersonation. In *Book Social Engineering in Social Networking Sites: The Art of Impersonation* (pp. 797-804).

[10] Algarni, A., Xu, Y., Chan, T., & Tian, Y. C. (2014). Social engineering in social networking sites: How good becomes evil. In *Book Social Engineering in Social Networking Sites: How Good Becomes Evil (The Association for Information Systems (AIS), edn.).*

[11] Algarni, A., Xu, Y., & Chan, T. (2015). *Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook.*

[12] Algarni, A., Xu, Y., & Chan, T. (2016). Measuring source credibility of social engineering attackers on Facebook. In *Book Measuring Source Credibility of Social Engineering Attackers on Facebook* (pp. 3686-3695).

[13] Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems* (pp. 1-27).

[14] Abu-Nimeh, S., Chen, T., & Alzubi, O. (2011). Malicious and spam posts in online social networks. *Computer, 44(9),* 23-28.
[15] Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. *International Journal of Information Management, 34(6),* 761-769.
[16] Hogben, G. (2007). Security issues and recommendations for online social networks. *ENISA Position Paper,* 1.
[17] Weiss, S. (2009). Privacy threat model for data portability in social network applications. *International Journal of Information Management, 29(4),* 249-254.
[18] Mohebzada, J., El Zarka, A., & Bhojani, A. (2010). *COE444 Spring 2010: Research Project Report.*
[19] Cutillo, L. A., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *Communications Magazine, IEEE, 47(12),* 94-101.
[20] Qi, T. (2007). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *Book An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering* (pp. 152-159).
[21] Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decision and Negotiation, 13(2),* 149-172.
[22] Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *Journal of Computing Sciences in Colleges, 26(2),* 80-87.
[23] Marett, K., Biros, D. P., & Knode, M. L. (2004). Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training. *Intelligence and Security Informatics,* 187-200.
[24] Bezuidenhout, M., Mouton, F., & Venter, H. (2010). Social engineering attack detection model: SEADM'. In *Book Social Engineering Attack Detection Model: SEADM'* (pp. 1-8).
[25] Twitchell, D. P. (2006). Social engineering in information assurance curricula. In *Book Social Engineering in Information Assurance Curricula* (pp. 191-193).
[26] Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others. *Information Management & Computer Security, 20(1),* 18-28.
[27] Peltier, T. R. (2006). Social engineering: Concepts and solutions. *EDPACS, 2006, 33(8),* 1-13.
[28] Mitnick, K. D., & Simon, W. L. (2001). *The Art of Deception: Controlling the Human Element of Security.*
[29] Gragg, D. (2003). A multi-level defense against social engineering. *SANS Reading Room,* 13.
[30] Nohlberg, M. (2008). *Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks.*
[31] Cialdini, R. B. (2001). *Influence: Science and Practice.* Boston: Allyn & Bacon.
[32] West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The weakest link: A psychological perspective on why. *Social and Human Elements of Information Security: Emerging Trends.*
[33] Simons, D. J., & Chabris, C. F. (1999). Gorillas in our midst: Sustained inattentional blindness for dynamic events. *Perception, 28(9),* 1059-1074.
[34] Noë, A. (2004). *Action in Perception.*
[35] Denzin, N. K., & Lincoln, Y. (2000). Qualitative research. *Thousand Oaks UA.*
[36] Creswell, J. W. (2012). *Qualitative Inquiry and Research Design: Choosing among Five Approaches.*
[37] Wolcott, H. F. (1994). *Transforming Qualitative Data: Description, Analysis, and Interpretation.*
[38] Gobo, G., & Marciniak, L. T. (2011). Ethnography. *Qualitative Research, 3(1),* 15-36.
[39] Emerson, R. M., Fretz, R. I., & Shaw, L. L. (2001). Participant observation and fieldnotes. *Handbook of Ethnography,* 352-368.

[40] Mulhall, A. (2003). In the field: Notes on observation in qualitative research. *Journal of Advanced Nursing, 41(3),* 306-313.

[41] Gold, R. L. (1958). Roles in sociological field observations. *Social Forces,* 217-223.

[42] Matavire, R., & Brown, I. (2008). Investigating the use of grounded theory in information systems research. In *Book Investigating the Use of Grounded Theory in Information Systems Research* (pp. 139-147).

[43] Algarni, A. A. M. (2016). The impact of source characteristics on users' susceptibility to social engineering victimization in social networks. *Queensland University of Technology,* 2016.

[44] Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*.

[45] Ekman, P. (2007). Emotions revealed: Recognizing faces and feelings to improve communication and emotional life. *Holt Paperbacks.*

[46] Cialdini, R. B., Wosinska, W., Barrett, D. W., Butner, J., & Gornik-Durose, M. (1999). Compliance with a request in two cultures: The differential influence of social proof and commitment/consistency on collectivists and individualists. *Personality and Social Psychology Bulletin, 25(10),* 1242-1253.

[47] Posey, C., Roberts, T., Lowry, P. B., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *Mis Quarterly, 37(4),* 1189-1210.

[48] Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51(5),* 551-567.

[49] Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Mis Quarterly, 39(1),* 113-134.

[50] Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *J. Assoc. Inf. Syst, 15(10),* 679-722.

[51] Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24(1),* 61-84.

[52] Wang, J., Gupta, M., & Raj, R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *Management Information Systems Quarterly*, *39(1),* 91-112.

Abdullah Algarni is currently an assistant professor in the Division of Information Technology, Institute of Public Administration (IPA), Saudi Arabia. He was previously with Queensland University of Technology (QUT), Australia. He received his Ph.D in computer science from Queensland University of Technology, Australia, and received the master degree in computer science from Western Michigan University, United States, and bachelor degree in computer science from King Abdulaziz University, Saudi Arabia. He published several papers in top information systems journals and conferences. His current research interests are mainly in the area of social engineering, phishing, deception, and information security management.