ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20220124142802

Preliminary communication
Received: 2022-01-24, Accepted: 2022-02-02

Social Media Security Awareness in Saudi Arabia

Musleh Alsulami

Abstract: With the daily use of social media, the cybersecurity and privacy are challenging for most communities. This research is aimed to explore and evaluate the awareness of cybersecurity in Saudi Arabia. It is also designed to discover how the ordinary users performances in using internet security while using social media. This research employed mixed methods. The researcher sent the online questionnaire to random people who used the social media to participate in this study. At the end of the online survey, one more question was attached to ask participants to involve in the second round of data collection (interview). This research found that social media users' awareness about internet security is different from users based on their gender. In addition, the ways of contact were affecting the reaction of users to share their information with others. The results also indicated that when the level of awareness is high the way of dealing with others is different. This study also confirmed the users' belief in internet security and most of them knew the strengths of internet security enabled them to protect their devices and personal information from outside intruders. Moreover, the findings of this study showed that the users of social media need to give more attention to all types of security threats. The findings of this paper can be used theoretically and practically by identifying the level of security awareness based on social media usage and the purpose of use.

Keywords: awareness; Saudi Arabia; security; social media

1 INTRODUCTION

Today, ensuring the privacy of your confidential information online is quite a challenge. The line between what is safe and what is not is quite thin these days. We have to take caution over the growing number of threats in the online space, from trojan horses to worms to viruses to spam even cyberstalkers. This study focused on three cyber threats which are widespread currently [14, 1]. Based on a research conducted in June 2012 by Mcafee.com the total number of malicious websites/bad URLs was more than 36 million. Moreover, the number of new bad URLs in a month was at over 2.7 million. The malicious websites are developed to infect your device with Trojan horses or and keystroke loggers. These malware are designed to collect critical personal information for example, credit card details and bank details [4]. If you do not take caution, these cyber criminals will get away with everything you possess [15]. Moreover, email security awareness is something crucial [27]. According to k-state.edu, this is another area that attackers use to launch cyber attacks. Some of the potential malware entry points when using E-mail include: adware, scams, attachments, spyware, bad URLs and viruses [11]. Prevention is better than cure, do not share personal information with anyone online. If you receive email messages from senders you cannot verify, do not open them. Owing to the ever-increasing complexity of cyberattacks, email scams can even collect your private and confidential data [18].

Today the easiness of networking socially is higher than before. However, this increased easiness comes with corresponding increased security risks [26]. Social networking platforms have continually shaped the behaviour of human beings [28]. Over the years, the amount of personal information that is shared online has been on the rise [9]. A common tendency in people is to share more personal information on the various social media platforms than with our families and friends [25]. Cyber criminals are taking note of this tendency in people and are continually taking advantage of this. Such personal information that is shared online can be used to social engineer the said people [11]. Avoid oversharing online, it is more dangerous than confiding in family and friends. The same risk of having your personal information stolen is as prevalent on these sites as anywhere else [3]. The possibility of cyber stalkers breaking into your homes or of pedophiles stalking your children cannot be ignored [10]. With this in mind, social network platforms may be regarded as the worst threats in IT world [1]. According to a prediction by Canada, in coming years Facebook will be the biggest threat to cybersecurity [24, 23]. IT World magazine did a SWOT analysis as well on the evaluation of security needs [20]. Here are some of the highlights below.

The security strengths of the organization include? In the case of organizations that are small, their strength can be deemed to be the fact they are small, therefore easier to secure compared to the larger companies. The presence of an existing security culture embedded in the companies systems is another strength [1]. It is easier to strengthen an organization with an already existing security infrastructure than one without. On the other hand, Lack of a culture that fosters security awareness or a program that does the same is regarded as a weakness [1]. For example, the lack of a well-defined patch management program is a sure shortcoming. However, companies that lack this have a huge opportunity to make amends and improve on this. In some instances, some organizations have been attacked due to existing minor vulnerabilities that would not have been exploited if there was a robust patch management system [2]. Bringing to reality a patch management program may be costly. However, this amount compared to the damage cost due to the existence of the vulnerability cannot be compared. Some weaknesses may be more technical than others [11]. The absence of a proper logging framework in place is a weakness that is easy to fix. Lack of funds is another prevalent weakness. Without funds, some weaknesses are hard to sort

out. In some cases, some organizations are put out of business following security breaches.

The security and protection of the Internet represents a great responsibility on the user to save his data, and this topic is related to our lessons in college in terms of the possibilities of networks and ways of connecting and securing. From our sense of the problem of safety on the internet we did this research to answer some of the questions which are:

1. What internet security characteristics are commonly published in social media discussions?
2. What are the similarities in the strategies of discipline in the sites of the wall on the social communication security methods?
3. What are the variations in disciplinary techniques in the social media's wall publications by internet security?

The aim of undertaking this study is:

1. Determine the security characteristics that are commonly published in social media
2. Investigation the similarities in the strategies of discipline in the sites of the wall on the social communication security methods
3. Discuss variations in disciplinary techniques in the social media's wall publications by internet security

The scope of this research was on the study of safety factors used by users on social networks. Moreover, this research was limited to the topic of internet security in social networking sites and did not address various internet sites, especially electronic payment methods, and this is under the ban on citizens due to the Corona virus with the frequent use of buying and selling through different internet sites.

2 MATERIAL AND METHODS

The presence of internet security in social media and how to develop this behaviour: this statement formed the basis of this study intending to examine the magnitude and nature of internet security use by human (even male or female) in social media. This study comes in handy for every researcher interested in people's internet security behaviour over social media and who are developing these behaviors of security. Denzin [8] state that the research design of a study refers to a set of guidelines linking theoretical models to practical methods of inquiry in addition to strategies for gathering empirical material; these guidelines can be adapted. So as to enable the collection of more complex data [17] suggests that the methodological system of the research be more qualitative. The underlying defense for this framework is the fact that the research tries to comprehend the cultural responses as well as the social semiotics internet security in social media. Hence, the current research adopts a qualitative approach, which means evaluating the answers of the respondents elicited through the interviews and focus groups, and making conclusions based on the subjective evaluation in addition to the analysis of the internet security in social media materials [12].

The aim of this research was to understand and evaluate the use of internet security in social media. Moreover, how their performances in using internet security at social media conversations? The researcher selected the sample by sending an online questioner to the most human that used social media (such as: Facebook, Twitter, Second Life, What's App), to answer if they use disciplinary in chatting with friends or formal chatting, and decided if they want to participate in the research. In the end of online survey (questionnaire), one more question is attached to ask participants for continuing the following interview protocol.

This study consists of two instruments and two stages:

1. Online survey of to see how they use internet security in conversations.
2. Online interview for discover how they evaluate the kind of internet security disciplinary they use on conversation (friendly or formal).

The researcher gathered spontaneous and unguided emerging information that was needful in coming up with subject matters for the facts. The goal of the researcher was to study the various degrees of internet security measures employed in social media. This was carried out with a goal to get insights on the role played by gender in internet security techniques. The researcher took up the role of a passive observer through out the interaction. This meant that the researcher could not get involved in any of the forums. However, he looked at the chosen social media platforms (Facebook page, Twitter, Second Life as well as What's App). While on the various platforms he was able to monitor the internet security patterns and the role of gender with regards to internet security techniques while using social media platforms.

The data collected, such as communication data, was subjected to close analysis at some point to notice internet security patterns during the commentary. With this in place, the researcher could have a more well defined view of the existing patterns as well as correlations between employed internet security techniques and gender on social media platforms. Later, this records become coded into a desk in step with Brown's and Levinson's (2005) internet security classes to get a more concise and more vast comprehension of internet security patterns. Moreover, the internet security measures to be applied based on social media usage will be more clear [22].

In the first stage (online survey), the participants will be of mixed gender (male and female) and will be approximately 40 participants (n = 40). The researcher will select the samples using convenient sample, by sending an online questionnaire in electronic versions with the informed consent letter and information statement simultaneously. Along with invitation participation to decide if they are willing to participate in the research. If participants complete the online questionnaire, one more question will be attached to ask them for continuing the following interview protocol. In the second stage (online interview), an online interview protocol will be used to collect data of participants to see how they evaluate the kind of internet security that they used. The interview protocol will be developed using the responses from the trends of online survey questionnaire. Analysis of the collected data was done using the following methods:

information records coding and categorizing. The statistics that were gathered were noted penned down in English. Next, the statistics was coded and categorized consistent with the types of internet security. Moreover, the language patterns from both male and girl contributors had been analyzed based totally on [14] concept. The system was able to successfully notice convergent as well as divergent patterns in the internet security practices of various genders. The system was able to construct tables that showed the correlation between the tendency of a given style of language and the employment of various internet security measures in the selected people's social media communications.

Tabs. 1-7 have been designed to show the frequency of language styles as well as the use of internet security schemes inside the social media forums of the chosen individuals. In the technique of coding, the transcribed discourse changed into segmented and categorized, consistent with Brown's and Levinson's (2005) theory of internet security techniques. Eventually, at the final degree of analyzing, this statistics were analyzed as a good way to pick out the goal of the communicators. Using coding manner was to generate an outline of categories of issues for analysis [7].

a) Statistical method

The study shall utilize several statistical methods, including standard deviation, mean as well as skewness and kurtosis(measures of normality), to obtain study results.

i) The Mean Eq. (1)

To obtain the mean, you divide the sum total of a given set of numbers by the size of the set. Most times, when people occasionally make mention of average, they are usually referring to mean. Calculations of mean come in handy in our daily lives. Using mean, you can find how long it takes you to get a job daily as well as find your average monthly expenditure.

$$M = \frac{1}{N}\sum_{i=1}^{N} a_i = \frac{1}{N}(a_1 + a_2 + \ldots + a_n). \quad (1)$$

ii) Standard Deviation Eq. (2)

The formula for finding the standard deviation is similar to the formula for finding the variance. It is the standard deviation formula is similar to the variance formula.

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2}. \quad (2)$$

Where: σ - standard deviation, x_i - each value of the dataset, $\overline{x}$ - the arithmetic mean of the data, N - the total number of data points, $\sum(x_i - \overline{x})^2$ - the sum of $(x_i - \overline{x})^2$ for all data points.

iii) Skewness Eq. (3)

Skewness is defined as a probability distribution measure of a random variable that is real-valued. Skewness assumes three possible types of values: negative, positive, undefined. A positive value of skewness means that the right side tail is longer than the left side tail and most of the values in the set occur to the left of the mean value. On the other hand, a negative skew means that the left side tail is longer than the one on the right. Moreover, a notable subset of the set occurs on the left side of the mean. A zero value means that there is a relatively constant distribution of the values on both ends of the mean value. However, this does not mean it's asymmetric distribution.

$$Skewness = \frac{\sum(M - a_n)}{\sigma}. \quad (3)$$

Where: M - the mean, a_n - sample number, σ - Standard deviation.

iv) Kurtosis (Eq. (4)

Using kurtosis, you get to know your graph's peak, that is, how high the graph is around the mean. This is regarded as the fourth moment in statistics. There are two possible values in this case: positive values and a negative value. If you obtain a positive value, it means you have little on your tails. If you obtain negative values, it means you have a lot of data on your tail. Lightness or heaviness of the tails depicts how peaked your data is, that is, more peaked for heavy and less peaked for light.

$$K = \frac{n(n+1)(n-1)\sum_{i=1}^{n}(x_i - M)}{(n-2)(n-3)\left(\sum_{i=1}^{n}(x_i - M)^2\right)^2}. \quad (4)$$

The quantitative survey data will inform the qualitative interviews, and this will lead to interpretation and help to shape the interview questions. Nvivo used to analyze the qualitative data.

3 RESULTS AND DISCUSSION

The extremely trendy social media application that the participants visit regularly shown in Tab. 1. About 50.00 % of the total participants agreed that they use all of the social media sites regularly. Only 15 people (37.50 %) mentioned that they utilize Facebook for general social media purposes. This study points out the widespread use of various social media platforms among the population for a number of varied reasons. This indicates the prevalence of communication sites among the majority of society.

The main purpose for regular browsing that the participants visit regularly shown in Tab. 2.

While replaying this item, 37 participants answered that they use chatting sites such as Facebook, Twitter, Second

Life, and What's App only for communication and chatting. The rest of the elements appear to be compatible with ratios in terms of study, games, and none with 1 for each category. Chung [6] and Cavalli [5] also mentioned that a great number of people access social media with the aim of chatting and communicating only. The useful tool for internet security among social media are shown in Tab. 3.

Table 1 Social Media Application

Type	Participants	Percentage, %
Facebook	15	37.50
Twitter	1	2.50
Second Life	2	5.00
What's App	2	5.00
All of them	20	50.00

Table 2 Purpose of Social Media Usage

Type	Participants	Percentage, %
Chatting	15	92.50
Study	1	2.50
Fun & Games	2	2.50
None	2	2.50

Table 3 Language Acquisition

Type	Participants	Percentage, %
Strong Agree	5	12.50
Agree	30	75.00
Disagree	5	12.50
Strong Disagree	0	0.00

Among all, 30 participants agreed that social media sites were useful for internet security, where 5 participants believed they strongly agreed. Five of them disagreed with this since this had never come to their knowledge. Consequently, a large number of participants supposed that social media could be valuable and safe by using internet security. McBride [16] points out the role played by various social media platforms to recreate changes in internet security. Tab. 4 shows the preferred mode of communication among social media users while on social media platforms.

Table 4 Communication Application

Type	Participants	Percentage, %
Chatting	32	80.00
Video Calling	4	10.00
Posting	4	10.00
Blogging	0	0.00

Thirty-two of the selected participants preferred communicating on social media platforms via chat. Four of these in the set said they prefer video calls as a mode of communication. In another case, 4 said they preferred to communicate with one another through posts, that is, by coming up with posts as well as commenting on other people's posts. Blogging as a mode of communication, in this case, did not interest anyone. Tab. 5 shows the user responses to the question, "Has usage of internet security in blogging or chatting affected the way your write academic papers or exam script?"

Table 5 Internet Security Programs

Type	Participants	Percentage, %
Yes	3	7.50
Often	15	37.50
No	15	37.50
Never	6	15.00

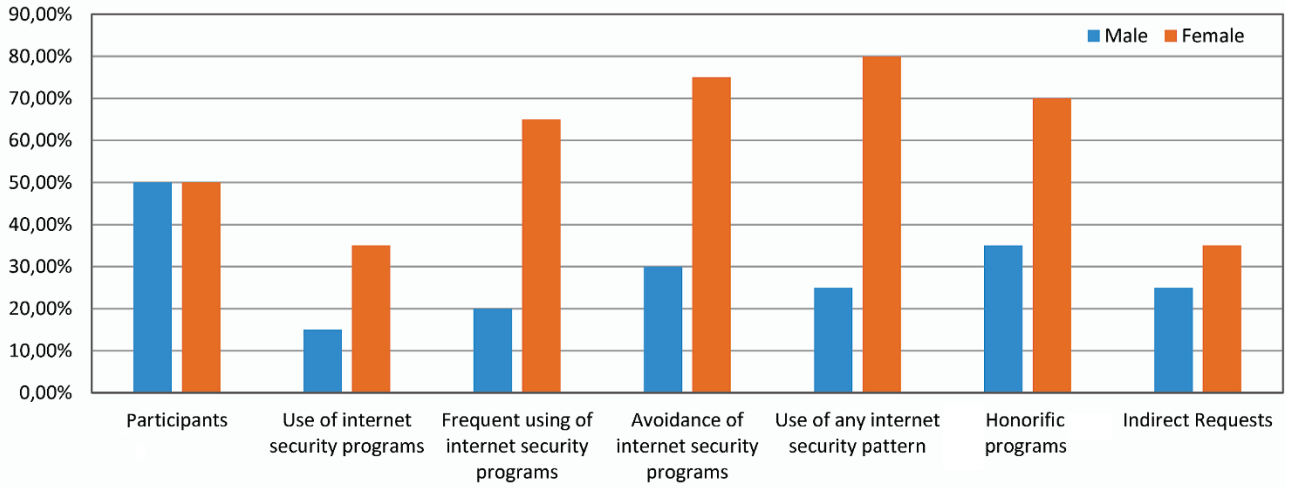

Figure 1 Internet Security Patterns

Including all 18 participants (7.15 % + 37.50 %) said that they got adopted by social media through using internet security programs in the practical life, where the other half (37.50 % + 15.00 %) said they avoid that condition regularly. Once over, these results encouragement the division between the conclusions of [21, 5]. This also provisions the indication of where the instigators stated that investigates had variations in results for having variability in reason, members, satisfied and background [19]. The regularity amount on the internet security programs patterns in social media's conversations of certain participants was shown in Tab. 6 and in Fig. 1.

The evaluation indicates that out of 20 male individuals, handiest three or 15.00 % of them tend to use extremely internet security of their social media's conversations. 4 or 20.00 % of male participants generally tend to internet security frequently, six of the male contributors (30.00 %) keep away from the use of internet security and use the

honorific program in their social media's conversations to reveal internet security. The Simplest 5 or 25.00 % of male individuals use tag questions, and some other 5 who represent 25.00 % of male participants generally tend to make requests from their pals circuitously in their social media conversations. Otherwise, out of 20 female individuals, 7 or 35.00 % of them use the extremely good-well-mannered shape of internet security and indirect requests in their social media safety programs. 14 or 70.00 % of those female participants use honorific programs, and 13 female with 65.00 % use safety and security also are discovered to have the tendency to more internet security via social media. A majority of 15 or 75.00% of the lady members keep away from the usage of any program for security at the same time as 16 female or 80.00 % of those female contributors use tag hack programs in their social media's security.

Table 6 Language Patterns

	Frequency of Usage		Percentage of usage (%)	
	Male	Female	Male	Female
Participants	20	20	50.00	50.00
Use of internet security programs	3	7	15.00	35.00
Frequent using of internet security programs	4	13	20.00	65.00
Avoidance of internet security programs	6	15	30.00	75.00
Use of any internet security pattern	5	16	25.00	80.00
Use of Honorific programs	7	14	35.00	70.00
Indirect Requests (Hack program)	5	7	25.00	35.00

The regularity amount on the use of internet security in social media's conversations of certain participants shown in Tab. 7 and in Fig. 2.

Table 7 Level of Internet Security

Internet Security Strategies	Frequency of Usage		Percentage of usage (%)	
	Male	Female	Male	Female
Programs	18	17	90.00	85.00
Online Software	8	13	40.00	65.00
Hack Programs	7	15	35.00	75.00
IP change	5	9	25.00	45.00

Internet security from different cultural histories might also define security in a distinctive way that is suitable to their context and settings [2]. In keeping with [13], Internet security is developed by using protocols and codes so as to reduce friction in private communications (1992) says politeness is the set of social values that communicators don't forget each different by way of gratifying shared expectancies. Consequently, it can be visible that humans exercise Internet security because there are desires for one to recollect their feelings, set up a given standard of mutual consolation as well as foster rapport.

The information evaluation has recognized numerous internet security patterns that are utilized by contributors in the various social media forums irrespective of gender. The accumulated information has been categorized based on Lakoff's (1975), Bonvillain's (2002), and Beeching's (2012) principle of internet security and gender, which encompass: using internet security form of safety, frequent using of internet security programs, internet security programs, use of any internet security pattern, use of honor program and indirect requests / hack program [10].

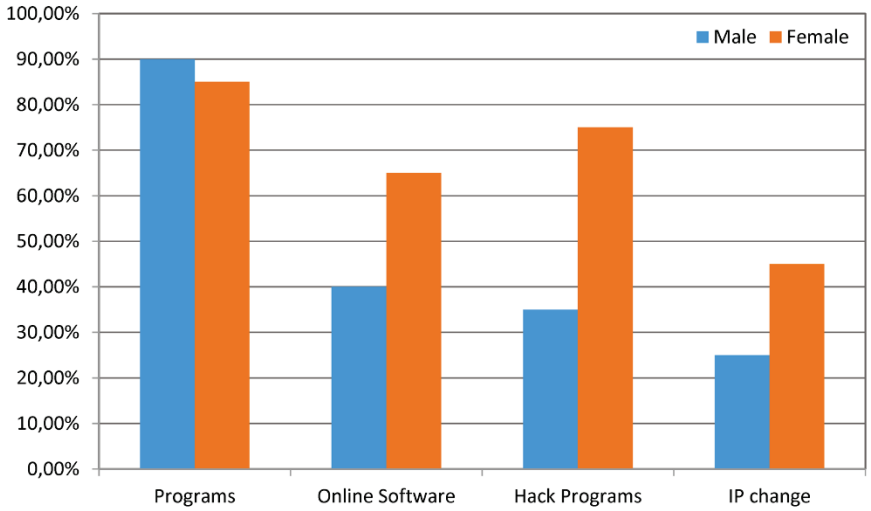

Figure 1 Level of Internet Security

Including all 18 participants (7.15 % + 37.50 %) said that they got adopted by social media by using internet security programs in practical life, where the other half (37.50 % + 15.00 %) said they regularly avoid that condition. Once over, these results encouragement the division between the conclusions of [21, 5]. This also indicates [19] where the instigators stated that investigates had variations in results for variability in reason, members, satisfied and background.

Except for the application of internet security techniques, male and woman also are determined to be exclusive in phrases of internet security sample. Lakoff [13] idea on female's language observed that girls are extra internet security than guys of their speech. Lakoff [13] proposed that ladies' language may be differentiated from men's through looking into some components along with using internet security, the avoidance of internet security thru first rate-

well-mannered shape consisting of they are using these programs and so on. Additionally, they express regret to a higher level as well as take pleasure in utilizing indirect request(s) while inquiring for assistance.

4 CONCLUSION

This study is helping in understanding the level of security awareness during the usage of social media in Saudi Arabia. The results indicated that there was no clear picture of information security in the minds of social media users. It is also indicated the level of awareness is varied from male to female about the term of "information security". The study contributed in two ways, theoretically and practically. From a theoretical point of view, this study would bridge the gap in the lack of literature within Saudi Arabia regarding security awareness in the usage of social media. From a practical point of view, this recommends the necessity to raise awareness of the importance of information security and safety.

5 REFERENCES

[1] Ahmad, N. et al. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication, 35*(2). https://doi.org/10.17576/JKMJC-2019-3502-29

[2] AlMindeel, R. & Martins, J. T. (2020). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology & People*. https://doi.org/10.1108/ITP-06-2019-0269

[3] Alzahrani, A. & Alanzi, T. (2019). Social media use by people with diabetes in Saudi Arabia: a survey about purposes, benefits and risks. *Diabetes, metabolic syndrome and obesity: targets and therapy*, 12, p.2363. https://doi.org/10.2147/DMSO.S208141

[4] Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon, 7*(1), p.e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

[5] Cavalli, N. C. (2011). *Facebook Influence on University Students' Media Habits: Qualitative Results from a Field Research*. Milan: University of Milan-Bicoca.

[6] Chung, K. S. (2015). Towards a Social Networks Model for Online Learning & Performance. *Journal of Educational Technology & Society*, 240-253.

[7] Creswell, J. (2013). *Qualitative, Quantitative and Mixed Method Approaches*. Great Britain. SAGE.

[8] Denzin, N. K. (2011). *The SAGE handbook of qualitative research*. SAGE, 45-52. https://doi.org/10.1177/1035719X1101100208

[9] Gharieb, M. E. (2021). Knowing the Level of Information Security Awareness in the Usage of Social Media Among Female Secondary School Students in Eastern Makkah Al-Mukarramah-Saudi Arabia. *International Journal of Computer Science & Network Security, 21*(8), 360-368.

[10] Hadlington, L., Binder, J., & Stanulewicz, N., (2020). Fear of missing out predicts employee information security awareness above personality traits, age, and gender. *Cyberpsychology, Behavior, and Social Networking, 23*(7), 459-464. https://doi.org/10.1089/cyber.2019.0703

[11] Hafid, A. & Sudyana, D. (2019). Analysis of Security Awareness in using Technology and Social Media at Muhammadiyah University of Riau. *International Journal of Computer Applications*, 975, p. 8887.

[12] Kothari, C. R. (2004). Research methodology: Methods and techniques (2nd revised ed.). *New Age International*, 52.

[13] Lakoff, R. (2018). *Internet Security—A Brief Review*. Great Britain: Cambridge University Press.

[14] López, J. (2017). Internet security. Paakat, 12-25.

[15] Malekian, R. (2020). Industrial Internet: Security, Architectures, and Technologies. IEEE Transactions on Industrial Informatics, 21- 30.

[16] McBride, K. (2009). Social-Networking Sites in Foreign Language Classes: Opportunities for re-creation. *American Journal of Education*, 35-58.

[17] Mills, K. A. (2009). Multiliteracies: Interrogating competing discourses. *Language and Education, 23*(2). https://doi.org/10.1080/09500780802152762

[18] Naughton, K. (2016). *Internet Security*. New York: Pearson.

[19] Oshima, J. O. (2012). Knowledge Building Discourse Explorer: a social network analysis application for knowledge building discourse. *Educational Technology Research and Development*, 903-921. https://doi.org/10.1007/s11423-012-9265-2

[20] Pulido, M. A., Johnson, C. W., & Alzahrani, A., (2021). Security Awareness Level Evaluation of Healthcare Participants Through Educational Games. *International Journal of Serious Games, 8*(3), 25-41. https://doi.org/10.17083/ijsg.v8i3.459

[21] Sallabank, J. (2010). The Role of Social Networks in Endangered Language Maintenance and Revitalization: The Case of Guernesiais in the Channel Islands. *Anthropological Linguistics*, 184-205. https://doi.org/10.1353/anl.2010.0011

[22] Pappas, C. et al. (2019). Network Transparency for Better Internet Security. *IEEE/ACM Transactions on Networking, 27*(5), 2028-2042. https://doi.org/10.1109/TNET.2019.2937132

[23] Van der Schyff, K. & Flowerday, S. (2021). Mediating effects of information security awareness. *Computers & Security*, 106, p.102313. https://doi.org/10.1016/j.cose.2021.102313

[24] Walker, J. (2014). Internet Security. Research Gate, 26-32. https://doi.org/10.1016/B978-0-12-416689-9.00007-1

[25] Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88, p.101640. https://doi.org/10.1016/j.cose.2019.101640

[26] Zeebaree, S., Ameen, S., & Sadeeq, M. (2020). Social media networks security threats, risks and recommendation: A case study in the kurdistan region. *International Journal of Innovation, Creativity and Change*, 13, 349-365.

[27] Zolait, A. H. S., Al-Anizi, R. R., Ababneh, S., BuAsalli, F., & Butaiba, N. (2014). User awareness of social media security: the public sector framework. *International Journal of Business Information Systems, 17*(3), 261-282. https://doi.org/10.1504/IJBIS.2014.064973

[28] Zwilling, M. et al. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1-16. https://doi.org/10.1080/08874417.2020.1712269

Author's contacts:

Musleh Alsulami, Dr.
Information Systems Department,
Umm Al-Qura University (UQU),
Makkah, Saudi Arabia
E-mail: mhsulami@uqu.edu.sa
https://orcid.org/0000-0003-4012-553X