ORIGINAL SCIENTIFIC RESEARCH

FAMILY MEMBER'S AWARENESS OF CYBER-SECURITY CONCEPTS AND ITS CORRELATION WITH THE PRECAUTIONARY PROCEDURES TAKEN AGAINST CYBER-ATTACKS DURING THE CORONAVIRUS PANDEMIC

MALIBARI Najat Abdullah[1]

[1]Housing and Institutions Management Department, Faculty of Human Sciences and Design, King Abdul-Aziz University, Jeddah, (Saudi Arabia)
e-mail: esfehani.mohamad3@gmail.com

ABSTRACT

This research aimed to explore the correlation between family members' awareness of cybersecurity concepts and the precautionary procedures taken against cyberattacks during the Coronavirus pandemic. A descriptive-analytical method was used. Also, a questionnaire was conducted to assess the correlation between family members' awareness of cybersecurity concepts and the precautionary procedure taken against cyberattacks during the Corona pandemic. The study sample consisted of 215 family members, males, females, employed and non-employed, students of different ages and educational levels. The results revealed a significant correlation between family member's awareness of cybersecurity concepts and the precautionary procedures taken against cyberattacks during the Corona pandemic. Besides, a significant difference ($p \leq 0.05$) in the family member's awareness level of the cybersecurity concepts, with some demographic variables (gender, employment status, age, education level, and average family income). Also, there was a significant difference ($p \leq 0.05$) in the preventive procedures taken by family members to protect themselves from cyberattacks with the study variables (gender, employment status, age, education level, and average family income).

Keywords: awareness, Corona pandemic, cybersecurity, cyberattacks.

JEL:M15

DOI: 10.5937/intrev2102122M

UDC: 004.738.5.056
004.738.5:316.362-047.22

COBISS.SR-ID 43513353

INTRODUCTION

The unprecedented increase in internet usage during the Coronavirus pandemic has never been witnessed before. Most family members have been using the internet a lot more to perform their jobs, attend educational classes, or for social purposes like reaching out to their acquaintances and friends. Studies published by the Ministry of Communication and the National Communication Institution (2020) have shown a significant increase in internet consumption among citizens reaching (89%) during the pandemic. Results indicated that there had been an increase of (376%) in educational sites, (131%) in internet sites, and (151%) increase in the usage of social media platforms such as Facebook. This explains why "personal internet users are increasingly exposed to security threats while using their home PC systems" [1]. "These personal internet users are becoming more vulnerable to security threats due to the use of information communication technologies" [1-3]. "In our technology and the information-infused world, cyberspace is an integral part of modern-day society.In both personal and professional contexts, cyber-space is a highly effective tool in, and enabler of, most people's daily digitally transposed activities". There is no pretension whatever that empowering proliferation of devices and information. Today the technology is far more available compare to yesterday and less than tomorrow [4][5][6].

The ease usage of technology with the elevated demand for online connectivity (in education, tourism, retail, and even autonomous vehicles) has developed internet usage opportunities globally. Several uses include utilizing search engines to find desired content, reading digital newspapers, surfing the web, using social media, assisting recommender systems in decision support tools, etc. However, the internet consumption bolster by information technology improvements increases dramatically [5], the information technology has elevated intensely in the past decade, with huge global internet consumption rates through individuals and organizations, ranging from academic and government to industrial sectors [6][7][8].

Governments can also adopt numerous means to spread cybersecurity awareness among family members by adopting effective means of communication with them; such as creating websites or pages on the internet, text messages, short films on YouTube, interactive games, television programs, educational advertisements using various advertising media platforms, holding conferences, courses and lectures in universities and schools, distributing brochures [9][10]. Including a description of the forms and types of crimes and dangers, and the concept of cybersecurity and its role in protecting family members and society from such attacks, and the procedures that individuals must follow to protect themselves and their families, and urges them to inform them of cybercrimes and not cover up the perpetrators by not reporting them [9][10][11].

Therefore, the researcher points out the importance of cybersecurity awareness between family members represented in the culture and etiquette of dealing with these technologies to achieve optimal results. It should also be their first defense line to protect themselves from cyberattacks, leaking their personal information and data, including the precautionary measures to protect all devices such as computers, mobile phones, and any smart device appliance from any possible cyberthreat.

The Norton Foundation for Studies indicated that crimes and cyberattacks in (2016) included (48%) of the total world population compared to (69%) in (2020), an increase of (21%), as a result of the steady rise in internet use in light of the Corona pandemic. "Kids and teens have embraced the digital world with great intensity, spending as many as eight hours a day online by some estimates" [12][13][14][15]. This emphasizes the urgent need for a qualitative shift in the mindset and thinking of technology users among family members to encourage them to take the procedural and precautionary measures necessary to secure their information and sensitive personal data from electronic attacks. It was discovered that (33%) of cybercrimes were aimed at businesses, while (77%) were directed at individuals [16][17].

Accordingly, the current research aims to study the awareness of cybersecurity concepts among family members to spread the culture of cybersecurity among community members to curb the increase in cybercrimes during the pandemic. Based on the related studies, we can consider these hypotheses for out study:

1. There are statistically significant differences between the awareness level of family members of cybersecurity concepts and the precautionary measures they take towards protecting cyberattacks during the pandemic.

2. There are statistically significant differences at ($p \leq 0.05$) in the level of awareness between family members of cybersecurity concepts due to personal variables (gender, employment status, age, educational level, and average household income).

RESEARCH METHODOLOGY

The research follows the descriptive-analytical method.

RESEARCH TOOLS

A questionnaire was used to assess thje level of cybersecurity awareness among family members and the relationship between that level of awareness and the precautionary measures taken to protect against cybercrime during the pandemic. The questionnaire contains two sections; the first one was to identify the research study sample variables (gender, age, educational level, average household income). Simultaneously, the second section was set to measure family members' awareness level with cybersecurity concepts and its correlation with the precautionary measures taken towards protection from cyberattacks during the pandemic.

RESEARCH LIMITATIONS

Objective limitations: The awareness level of family members of cybersecurity concepts and its correlation with the precautionary measures taken towards protecting from cyberattacks and social engineering during the pandemic.

Human limitations: The research study sample consisted of (215) family members, employed and non-employed, males and females, students of different ages, educational levels, and lastly, different household incomes.

Spatial limitations: Kingdom of Saudi Arabia, Makkah Al-Mukarramah region (Jeddah - Makkah - Taif).

Temporal limitations: Year (2020/1441).

RESEARCH PROCEDURES

The researcher followed the descriptive-analytical method that studied the discussed phenomenon as it is in real life. Besides, accurately describing and clarifying its characteristics by collecting information, analyzing and interpreting it to reach conclusions that contributed to understanding the essence. This was achieved by analyzing the phenomenon or problem to make concrete generalizations from which the analysis would enhance knowledge and understanding of the phenomenon.

QUESTIONNAIRE CONTENT VALIDITY

This refers to the questionnaire's ability to collect the requisite data and generate the desired results.

APPARENT CONTENT VALIDITY

The method of apparent content validity was used to ensure the questionnaire's validity and suitability for research purposes. This is done by presenting it to a team of six specialized academic arbitrators from King Abdul-Aziz's faculty members, and Taibah's University majored in information technology and cybersecurity. Who also have excellent knowledge and interest in the subject of this research. They were asked to assess and provide feedback regarding the validity and coherence of the questionnaire and its suitability to measure what it was set for and make the necessary amendments, whether by deleting, adding, or reformulating. The questionnaire has been amended and modified adhering to the arbitrators with the below adjustments:

First section amendments: questions number (13 & 21) have been removed, rephrased questions number (2, 10 17, 24 & 29), and merged questions number (9 with 13).

Second section amendments: questions number (2, 20, 30, 36, 37, 46 & 54) have been removed, rephrased number (44 & 51), and merged number (28 with 30) and (29 with 31).

*The amendments were made according to the feedback of two arbitrators or more.

Results were scored as:

Responses for the first section were scored as the following:

(1) for questions to which the answer is "no", and (2) for questions to which the answer is "yes" for questions of a positive nature. In contrast, the score (2) is given to the answer "no", and the score (1) to answers "yes" to questions of a negative nature.

While the responses for the second section were scored as the following:

(1) for questions to which the answer is "rarely", (2) for questions to which the answer is "sometimes", and (3) for questions to which the answer is "always" for questions of a positive nature. In contrast, the score of (3) is given to the answer "rarely", (2) for the answer "sometimes", and (1) for the answer "always" to questions of a negative nature.

The internal content validity method was applied to each section's total scores and the total score of the whole questionnaire to validate it.

INTERNAL CONTENT VALIDITY

Internal content validity means how each statement/question of the questionnaire is consistent and coherent with the section to which they belong. Accordingly, to validate the questionnaire, the correlation coefficients were calculated between each statement/question's scores and the section's total score to which they belong. The following results validate the internal content of the study tool:

The first section of the study tool consisted of (21) statements/questions. To ensure the internal content validity of these statements and how they presented the section of which they belong, the correlation coefficients between each statement/question and the section's total scores were calculated as shown in Table (1).

Table 1. First section's internal content validity

Statement number	Correlation Coefficient	Significance Level	Statement number	Correlation Coefficient	Significance Level
1	0.404**	0.000	12	0.361**	0
2	0.464**	0.000	13	0.384**	0
3	0.388**	0.000	14	0.342**	0
4	0.113	0.099	15	0.309**	0
5	0.000	0.996	16	0.422**	0
6	0.049	0.478	17	0.484**	0
7	0.491**	0.000	18	0.376**	0
8	0.510**	0.000	19	0.501**	0
9	0.371**	0.000	20	0.476**	0
10	0.513**	0.000	21	0.014	0.84
11	0.392**	0.000			

** Statistical value at (0.01). * Statistical value at (0.05)

It is evident from Table (1) that all statements/questions on the first section are correlated statistically at a level of significance of (0.05) with the total score of the section, with the exception for statement numbers (4, 5, 6 & 21). Correlation coefficients for the rest of the statements ranged between (0.309 and 0.513), indicating the existence of internal content validity and consistency between the statements/questions of the first section, which validate the data collected from the study sample in this regard.

CONTENT VALIDITY OF THE STATEMENTS/QUESTIONS OF THE SECOND SECTION

The second section of the study tool consisted of (38) statements/questions and to ensure the content validity of these statements/questions and how they presented the section to which they belong. The correlation coefficients between each statement/question and the section's total scores were calculated as shown in Table (2).

Table 2. Second section's internal content validity

Paragraph number	Correlation Coefficient	Significance Level	Paragraph number	Correlation Coefficient	Significance Level
1	0.389**	0.000	20	0.272**	0.000
2	0.328**	0.000	21	0.485**	0.000
3	0.442**	0.000	22	0.257**	0.000
4	0.371**	0.000	23	0.410**	0.000
5	0.326**	0.000	24	0.472**	0.000
6	0.406**	0.000	25	0.426**	0.000
7	0.390**	0.000	26	0.422**	0.000
8	0.374**	0.000	27	0.328**	0.000
9	0.332**	0.000	28	0.518**	0.000
10	0.400**	0.000	29	0.436**	0.000
11	0.409**	0.000	30	0.338**	0.000
12	0.388**	0.000	31	0.592**	0.000
13	0.446**	0.000	32	0.323**	0.000
14	0.364**	0.000	33	0.136*	0.046
15	0.350**	0.000	34	0.469**	0.000
16	0.406**	0.000	35	0.072	0.294
17	0.227**	0.001	36	0.371**	0.000
18	0.447**	0.000	37	0.539**	0.000
19	0.356**	0.000	38	0.322**	0.000

*** Statistical value at (0.01). * Statistical value at (0.05)*

It is evident from Table (2) that all statements/questions on the second section are correlated statistically at a level of significance of (0.05) with the total score of the section, with the exception for statement number (35), which has been excluded. Correlation coefficients for the rest of the statements ranged between (0.136 and 0.592), indicating the existence of internal content validity and consistency between the statements/questions of the second section, which validate the data collected from the study sample in this regard.

CONSTRUCTIVE VALIDITY

Constructive validity is one of the validity study tools, and it is defined as "the degree to which a test measures what it claims, or purports to be measuring." Table (3) showed the results of the constructive validity of each section of the questionnaire.

Table 3. Questionnaire's constructive validity

Section	Correlation Coefficient	Significance Level
1st	0.486	0.000
2nd	0.966	0.000

It is evident from Table (3) that both sections of the questionnaire are correlated statistically at a level of significance of (0.05) with the total score of the survey. Thus both sections of the questionnaire are constructively valid.

STUDY TOOL STABILITY

The study tools' stability has been achieved by applying both (Cronbach's Alpha) and (Split -Half) formulas. Table (4) showed the stability of the study tool for both methods.

Table 4. Stability of the study tool using (Cronbach's Alpha) and (Split -Half) formulas.

Section	Cronbach's Alpha Formula		Split-Half Formula	
	Number of Statements	Cronbach's Alpha Coefficient	Pearson Correlation Coefficient	Split-Half Coefficient
1st	21	0.605	0.379	0.55
2nd	38	0.819	0.708	0.828

It is evident from Table (4) that (Cronbach's Alpha) coefficient value for the first section's statements/questions representing the level of awareness of family members of cybersecurity concepts is (0.605), while the value of the (split-half) coefficient is (0.550). Whereas the second section representing the precautionary measures taken towards the protection from cyberattacks and social engineering (Cronbach's Alpha) coefficient value is (0.819) and of a (0.828) for the (split-half) coefficient value, indicating the validation of the data collected from the study sample in this regard.

STATISTICAL METHODS USED

The Social Statistical Package (SPSS ver. 21) was used for data processing with the necessary statistical methods to fulfill the study's aims. These methods were as follows:

Frequencies and Percentages: used to analyze personal and business data of the study sample.

Mean: used in substantive response extraction, strength discriminatory clauses. As well as to find means for computational research samples.

Standard Deviation: to identify the extent of the deviation of the responses of the study sample for each paragraph/statement from its mean. The more its value approaches zero, the reactions are concentrated, and their dispersion decreases.

Cronbach's Alpha and Split Half: to measure the stability of the study tool and data reliability.

Pearson Correlation Coefficient: to measure the internal content validity of the study, and to verify the correlation between family members awareness level of the concepts of cybersecurity and the precautions they take to protect themselves from cyberattacks & social engineering.

One Sample T-test: to verify the existence of statistically significant differences in the mean of the average responses of the study sample for each statement/question of the questionnaire, and the total score for each section.

T-test for two independent samples: to verify the existence of statistically significant differences in the responses of the study sample due to personal variables.

One-way ANOVA: to verify the existence of statistically significant differences in the responses of the study sample due to personal variables.

RESULTS AND DISCUSSION

The study sample consisted of (215) family members, residents of Makkah Al-Mukarramah region (Jeddah - Makkah Al-Mukarramah - Taif), where the study relied on the simple random sampling (SRS) method. At the same time, the questionnaire was conducted online. Table (5) showed the characteristics of the study sample according to initial data:

Table 5. Distribution of the study sample according to the primary data

Variable	Category	Number	Percentage %
Gender	Male	48	22.3
	Female	167	77.7
Employment status	Employed	160	74.4
	Non-employed	34	15.8
	Student	21	9.8
Age (Year)	Under 20	1	0.5
	20-30	31	14.4
	31-40	65	30.2
	41-50	67	31.2
	51-60	34	15.8
	Above 61	17	7.9
Educational Level	Intermediate	1	0.5
	High school or equivalent	6	2.8
	College degree	101	47
	Postgraduate degree	107	49.8
Economics level	Less than 3000 SR	6	2.8

	3000-7,000 SR	36	16.7
	7,000-10,000 SR	65	30.2
	More than 10,000 SR	108	50.2
Total		**215**	**100**

Table (5) showed the research study sample's distribution according to the study variables, which included (gender, employment status, age, educational level, and average household income). The majority of the study sample were females, with only (22.3%) males. Most of the study sample are employed with a percentage of (74.4%) and only (9.8%) were students. And as for the age variable, it is noted that (14.4%) their ages ranged between (20-30) years, (30.2%) their ages ranged between (31-40) years, (31.2%) their ages ranged between (41-50) years, (15.8%) their ages ranged between (51-60) years, and only (7.9%) are over (60) years old.

As for the educational level, it is noted that most of the study sample with a percentage of (49.8%) had a postgraduate degree, followed by a very slight difference for college degree holders where their percentage reached (47%). The percentage for secondary education or its equivalent among the study sample decreased to (28%). And as for the average household income (50.2%), their household income exceeds (10,000) SR, followed by (30.2%) for households with an income ranging between (7000:10,000) SR, and (16.7%) their household income goes between (3000:7000) SR. In comparison (28%) their household income is less than (3000) SR.

First hypothesis: “There are statistically significant differences between family members’ awareness level of cybersecurity concepts and the precautionary measures taken towards the protection from cyberattacks during the Corona pandemic.”

To test this hypothesis’s validity, the researcher used the Pearson correlation coefficient formula to disclose a statistically significant correlation between family members’ awareness level of cybersecurity concepts and the precautionary measures they take to protect themselves from cyberattacks and social engineering. This is evident from the following table:

Table 6. The correlation between family members’ awareness level of cybersecurity concepts and the precautionary measures taken towards the protection from cyberattacks and social engineering during the Corona pandemic

Family member’s awareness level of cybersecurity concepts and the precautionary measures taken towards the protection from cyberattacks and social engineering during the Corona pandemic	**Pearson’s Correlation Coefficient**	**Significance level**
	0.243	0.000

Table (6) showed a correlation between family members’ awareness of cybersecurity concepts and the precautionary measures they take to protect themselves from cyberattacks, as the values were statistically significant at a significance level (0.001). This indicates the validity of the hypothesis with an apparent correlation between the two halves of the study. According to the researcher’s point of view, those results affirm the need to increase the level of awareness and knowledge of cybersecurity between families and individuals; this will prompt the government to raise their citizen’s level of understanding by sharing the cybersecurity tips, broaden their knowledge of the concept and its efficient role in protecting individuals and institutions, using social media platforms which have proven itself to be the most efficient way of communication nowadays.

Second hypothesis: “There are statistically significant differences at the level of significance of ($p \leq 0.05$) between family member’s awareness level of cybersecurity concepts and the precautionary measures taken towards the protection from cyberattacks during the Corona pandemic, due to the study sample personal variables which included (gender, employment status, age, educational level, and average household income)”.

To verify the validity of the hypothesis, the researchers conducted the following statistical analyzes:

Student-t-test for two independent samples to verify the existence of statistically significant differences in the awareness level of family members of cybersecurity concepts of the study sample due to gender differences as shown in Table (7).

Table 7. Significant differences results of family members awareness level of cybersecurity concept due to the gender variable

Gender	Number	Mean	Standard Deviation	"t" Value	Significance Level
Males	48	1.66	0.197	1.563	0.12
Females	167	1.71	0.16		

It is evident from Table (7) that there are no significant differences in the awareness level of family members of cybersecurity concepts due to the gender variable, as “t” value was (1.563), which is greater than the level of significance which is at (5%). This indicates no significant difference in the awareness level of family members of cybersecurity concepts due to the gender variable.

The (ANOVA) test method has been used to analyze the single-sample variance of two independent samples to show the statistically significant differences in the awareness level of family members of cybersecurity concepts due to the employment status variable (employed, non-employed, student). Results are shown in Table (8).

Table 8. Significant differences results of family members awareness level of cybersecurity concept due to the employment status variable

Employment status	Number	Mean	Standard Deviation	“F” Value	Significance Level
Employed	160	1.7	0.166	0.24	0.787
Non-employed	34	1.69	0.171		
Student	21	1.72	0.202		

It is evident from Table (8) that no significant differences in the awareness level of family members of cybersecurity concepts was found due to the employment status variable, as “F” value was greater than the level of significance at level (5%). This indicates no significant differences in the awareness level of family members of cybersecurity concepts due to the employment status variable.

The (ANOVA) test method has been used to analyze the single-sample variance of two independent samples to show the statistically significant differences in the awareness level of family members of cybersecurity concepts due to the age variable. The results are shown in Table (9).

Table 9. Significant differences results of family members’ awareness level of cybersecurity concept due to the age variable

Age (Year)	Number	Mean	Standard Deviation	“F” Value	Significance level
Under 20	1	1.33	.	2.167	0.059
20-30	31	1.74	0.123		
31:40	65	1.68	0.168		
41-50	67	1.71	0.181		
51-60	34	1.72	0.161		
More than 61	17	1.64	0.192		

It is evident from Table (9) that there are no significant differences in the awareness level of family members of cybersecurity concepts due to the age variable, as "F" value was (0.059), which is greater than the level of significance which is at (5%). This indicates no significant difference in the awareness level of family members of cybersecurity concepts due to the gender variable.

The (ANOVA) test method has been used to analyze the single-sample variance of two independent samples to show the statistically significant differences in the awareness level of family members of cybersecurity concepts due to the educational level variable. The results are shown in Table (10).

Table 10. Significant differences results of family members awareness level of cybersecurity concept due to the educational level variable

Educational level	Number	Mean	Standard Deviation	“F” Value	Significance Level
Intermediate	1	1.33	.	3.146	0.026
High school	6	1.56	0.318		
University	101	1.71	0.16		
Postgraduate	107	1.7	0.164		

It is evident from Table (10) that there is a significant difference in the awareness level of family members of cybersecurity concepts due to the educational level variable, as "F" value was (0.026), which is less than the level of significance at (5%). This indicates a significant difference in family members' awareness level of cybersecurity concepts due to gender.

The (ANOVA) test method has been used to analyze the single-sample variance of two independent samples to show the statistically significant differences in the awareness level of family members of cybersecurity concepts due to the average household income variable. The results are shown in Table (11).

Table 11. Significant differences results of family members awareness level of cybersecurity concept due to the average household income variable

Economics level	Number	Mean	Standard Deviation	"F" Value	Significance level
Less than 3000 SR	6	1.86	0.117	5.563	0.001
3,000-7000 SR	36	1.61	0.29		
7,000-10,000 SR	65	1.72	0.125		
More than 10,000 SR	108	1.71	0.126		

It is evident from Table (11) that there is a significant difference in the awareness level of family members of cybersecurity concepts due to the average household income variable, as "F" value was (0.001), which is less than the level of significance at (5%). This indicates a significant difference in the awareness level of family members of cybersecurity concepts due to the average household income variable.

CONCLUSION

Based on the results obtained, it can be concluded that:

1- The concerned authorities' cooperation plays a crucial role in educating family members about new cybersecurity concepts, communication, and information technology.

2- Disseminating cybersecurity tips through the most effective means of communication to educate and train individuals to deal with cyberattacks in all of their forms and types.

3- Training family members on security measures, procedures and precautions that must be followed to protect themselves and their families from cyberattacks to reduce cyber-hacking risks due to the lack of awareness and knowledge of cybersecurity.

4- Specially designed educational awareness programs for high schoolers and college students to educate them about cybersecurity and use social media platforms safely.

5- Educating the youth and younger generations on how to deal with the strangers they face on the web through social media platforms or gaming applications.

6- Embed different cybersecurity concepts in the educational curriculums to suit all stages and grades.

7- Disseminating the method of reporting cyberattacks through all social media platforms to be easily reached by individuals.

REFERENCES

[1] Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), pp. 410-417. https://doi.org/10.1016/j.cose.2007.03.001.

[2] Sophos, (2009). The Sophos Security Threat Report, pp. 123-143.

[3] Dean, T., Stephen, E., Marci, D., Marc, F., Joseph, B., David, M., Ronald, B., Nicholas, S., Peter C., Candid, W., Ollie W. and Zulfikar, R. (2007). Symantec internet security threat report. Trends for January-June. 07. Vol. XII.

[4] Geer, D. (2015). Six key areas of investment for the science of cyber security. Futurist, 49(1), pp. 10-15.

[5] Maurseth, P.B. (2018). The effect of the internet on economic growth: counter-evidence from cross-country panel data. Econ Lett.,172, pp.74–77.

[6] Aloul, F. A. (2012). The need for effective information security awareness. Journal of advances in information technology, 3(3), pp. 176-183. https://doi.org/110.4304/jait.3.3.176-183.

[7] Lee, K. G., Chong, C. W., & Ramayah, T. (2017). Website characteristics and web users' satisfaction in a higher learning institution. International Journal of Management in Education, 11(3), pp. 266-283. https://doi.org/10.1504/IJMIE.2017.084926.

[8] Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. The Journal of Strategic Information Systems, 28(1), pp. 66-82. https://doi.org/10.1016/j.jsis.2018.09.003.

[9] Ahmed, R. (2014). The extent of parents' awareness of their roles aimed at promoting children's safety on the internet and the degree of their practice of it, Journal of Educational Sciences, P (1) Girls College of Arts and Sciences and Education, Ain Shams University.

[10] Antara, B.M. & Mohieddine, H. (2020). Cybersecurity as a new dimension in Algerian defense policy at the University of Mohamed Boudiaf, Messila, Faculty of Law and Political Sciences.

[11] Hall, C. (2012). Security of the Internet and the Known Unknowns. Communications of the ACM, 55(6), pp. 35-37. https://doi.org/10.1145/2184319.2184332.

[12] Kumar, N., Mohan, K., & Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. Decision Support Systems, 46(1), pp. 254-264. https://doi.org/10.1016/j.dss.2008.06.010.

[13] Erfani, A. O., Almasi, M., & Reshadatjoo, H. (2019). Evaluation of the Relevant Factors with the Formation of Marginalization in Qorveh, a Case Study in Sheikh Jafar Quarter. International Journal of Advanced Studies in Humanities and Social Science, 8(3), pp. 241-254. http://dx.doi.org/10.33945/SAMI/IJASHSS.2019.3.2.

[14] Mohammadkhani Orouji, F. (2021). Investigating the Relationship between Emotional Intelligence and Social Causes of Job Development in Working Children and Normal Children. Int. J. Adv. Stu. Hum. Soc. Sci., 10(1), pp. 1-6. http://dx.doi.org/10.22034/ijashss.2021.268820.1034.

[15] Soltani, Z. (2021). Comparative Study of the Laws Governing Contracts in Conflict of Laws in Iran and France law. International Journal of Advanced Studies in Humanities and Social Science, 10(1), pp. 22-32.http://dx.doi.org/10.22034/ijashss.2021.271226.1040

[16] Rahimipour, S. (2020). Poetry and Drama: A Survey of Their Applicability to Language Teaching/Learning. International Journal of Advanced Studies in Humanities and Social Science, 9(1), pp. 72-83.http://dx.doi.org/10.33945/SAMI/IJASHSS.2020.1.6

[17] Hashemi Fard, K. (2020). Proof of Ethics with Math. International Journal of Advanced Studies in Humanities and Social Science, 9(1), pp. 84-88. http://dx.doi.org/10.33945/SAMI/IJASHSS.2020.1.7

Article history:

Received 10 May2021

Accepted 1 July 2021