The Role of Secondary Education in Enhancing the Information Security Culture among Students in Saudi Arabia

Dr. Maher Ahmed Hassan

Foundations of Education Department - College of Education, Imam Abdulrahman Bin Faisal University, P.O Box 2375 , Dammam 31451, Saudi Arabia
Mamohamed@iau.edu.sa
Orcid id: https://orcid.org/0000-0001-8070-8129

Abstract:

The culture of information security is one of the important issues that have received the attention of all educational institutions, to educate students and inform them of the risks and threats they are exposed to while using the Internet. Thus, the study tries to identify the secondary education role reality in enhancing information security culture among students in Saudi Arabia, its obstacles, and the requirements to be activated. The study applied a questionnaire to a stratified random sample of (267) male and female teachers in secondary schools. The study concluded that the role of secondary education in enhancing information security culture among students is weak. In addition, there are significant obstacles that limit its role in enhancing information security culture among students. Hence, the necessary requirements must be provided to activate its role in enhancing information security culture among students. There are also statistically significant differences between males and females regarding the secondary education role reality in enhancing the information security culture and its obstacles in favor of females at the significance level ($\alpha \le 0.05$), in favor of males at the significance level ($\alpha \le 0.01$) in the requirements for enhancing the information security culture.

Keywords: Secondary Education, Information security Culture.

1. Introduction:

The contemporary digital revolution has created unprecedented prospects for communication and the exchange of information, ideas, and opinions among Internet users around the world. The use of the Internet has become available, with the spread of smartphones and mobile devices, to all society members of all age groups. Despite the great advantages of using the Internet in social communication and the completion of many transactions, a new threat appeared to those users, represented by hacking personal accounts, manipulating and stealing information, and harming users in multiple ways and methods, in what is known as cybercrime (Chang et al., 2013), which led to material, economic and social losses for both individuals and societies.

The preventive, personal and social protection aspects of the Internet and its various applications pose a challenge to users of all ages, especially the younger generations. This increases the demand for developing information security skills for those generations on the Internet. Despite the fact that most social networking sites and the Internet are dedicated to adults and older adolescents, the number of young teenagers and children joining the list of permanent users of these networks is constantly increasing day by day. Also, Al-huwaimel (2020) points out that by giving these children and adolescents an opportunity to join the Internet

and social networking, they are targeted by scams, harassment, and exposure to malware.

Due to the importance of information security for individuals and societies, many international authorities, such as UNESCO, the International Organization for Standardization (ISO), and the US Federal Government, have been interested in developing standards and laws for information security such as ISO/IEC 27001, ISO 27002, ISO 15408, ISO 13335, and the COBIT Stander, which was built by the Information Technology Governance Institute (ITIG) (Zaghloul & Shehata, 2019).

Many developed countries have also tended to adopt initiatives aimed at providing information security to all Internet users, especially school students, including the European Union initiative in 2009, which included the inclusion of information security concepts in school curricula in (24) European countries. In addition, the United States of America established the National Alliance for Security and the Ministry of Defense was responsible for promoting and spreading awareness of information security (Solms & Solms, 2015). Furthermore, the US government launched the National Initiative for Cyber Security Education (NICE) to prepare a workforce in the field of information security (Wilson, 2014). Information security aims at protecting information resources owned by individuals, institutions, and countries that are stored and circulated through the computer environment, of which hardware, software, and the Internet are the most important elements.

Martin et al. (2018) demonstrated that cyberbullying, digital identity, digital prints, and inappropriate social media use are topics of interest in general education schools. With the increasing number of schools and school districts implementing "Bring Your Own Technology initiatives", more attention is given to these topics.

The responsibility of spreading awareness of information security is related to educational institutions. A study, carried out by Rahman et al. (2020), indicated the importance of the role played by educational institutions in determining the extent of society's interest in issues related to information security. In this context, Goran (2017) emphasized the importance of raising the awareness level of students and teachers regarding information security and their protection from cybercrime that they may be exposed to while using the Internet. Also, Yilmaz et al. (2017) emphasized the importance of raising awareness of information security among secondary school students to face the threats and risks that exist on the Internet. Al-Montashari (2019) emphasized the importance of raising the awareness level of information security among students, teachers, and educational supervisors in schools.

Despite the Kingdom of Saudi Arabia's interest in spreading awareness of information security among individuals in the society, there are many studies confirming the weak awareness of information security among students in schools. The study of (Al-Manea, 2015; Sayed, 2015) confirmed that handling information security topics included in the computer course in secondary schools are below the required standard, and that the role of teachers in promoting behaviors related to information security is weak. The study of Al-Zahrani et al. (2020) indicated the lack of awareness of information security importance among students in Saudi schools. The study of Gharib & Al-Amir (2017) emphasized the weak awareness of information security among female students in the secondary stage, and found that (57%) of the female students do not set a password to protect their computers, and (41%) do not change passwords constantly for their personal accounts.

The widespread use of secondary school students to access the Internet via mobile devices and computers has exposed them to many risks and threats such as hacking their personal accounts, stealing and destroying their information, theft of their identity, and impersonation. In addition to being subjected to bullying and personal harassment, Internet addiction and social isolation, this caused them much material, psychological and moral harm. It imposes on secondary education the need to educate students and provide them with an information security culture to protect them from

those risks. Hence, the current study tries to identify the secondary education role reality in enhancing information security culture among students. The problem of the current study is determined by the following questions:

1. What is the secondary education role reality in enhancing information security culture among students in Saudi Arabia?

2. What are the obstacles to enhancing information security culture among secondary education students in Saudi Arabia?

3. What are the requirements for activating the secondary education role in enhancing information security culture among students in Saudi Arabia?

4. What are the statistically significant differences between teachers' responses in the secondary education role reality in enhancing information security culture among students, its obstacles, and its requirements for activation according to two variables: gender and years of experience?

This study is beneficial for officials in the Ministry of Education and secondary school principals to identify the secondary education role reality in enhancing information security culture among students and its obstacles, as well as the most important requirements that must be met to activate the role of secondary education in supporting information security culture to protect students from electronic risks and threats they are exposed to while using applications electronically inside and outside the school.

2. STUDY BACKGROUND:

2.1 Information Security Concept:

The issue of information security, at the present, has occupied the attention of all individuals, specialists and countries, due to the dependence of modern societies on information and communication technology connected to the global network, which is accompanied by a set of emerging and potential risks that threaten the global community and its individuals.

Whitman & Mattord (2017) defined information security as maintaining the confidentiality and integrity of information as an asset in the stages of processing, preservation, and transmission. This is achieved through the actual application of security policies and through the promotion of awareness, learning and training. Craigen, Diakun & Purse (2014) defined it as the process of organizing and assembling resources, processes and structures that enable cyberspace to stop intrusion in its various forms, which are carried out illegally. Information security was defined by Zagloul & Shehata (2019) as all measures and procedures that must be taken to protect the information system from internal and external threats to data, information, software and hardware, so as to achieve confidentiality, integrity and availability.

Hence, achieving information security protects society with all its institutions and members from risks that threaten its stability while using technological innovations in accordance with specific rules and controls. It also guarantees Internet users the security of data and information by not leaking it, protecting intellectual property, observing and respecting privacy, and taking all preventive measures to protect individuals in society from harmful and malicious data and information.

2.2 Information Security Aims:

Educational countries seek to enhance students' information security, awareness of the following aims (Al-Rabiah 2017; Martin & Whitmer, 2016; Saegh, 2018):

- Providing a safe environment for users with a great deal of reliability in the society of information.

- Enabling users to respond to information security attacks and incidents targeting their computer devices and personal data.

- Providing the necessary requirements to reduce cybercrime targeting users.

- Resisting malware and its severe damage to users and information systems.

- Strengthening the protection, confidentiality and privacy of users' personal data.

- Eliminating weaknesses in computer systems and mobile devices and filling gaps in information systems.

- Protecting users against potential risks in the various areas of Internet use.

- Enhancing the protection of operational technology systems and their hardware and software components, the provided services including data.

2.3 Information Security Culture:

Information security culture is one of the important issues that received the attention of all society institutions to educate individuals and inform them of the direct and indirect risks and threats they are exposed to during their dealings with electronic applications.

The information security culture is represented in all educational programs and activities offered by schools to educate their students about the importance of information and its preservation to protect themselves and society from the dangers that threaten them through attack. The information security culture includes three basic aspects:

2.3.1 Personal Information Security Culture: It is related to the user, his personal information, his behavior, and the way he deals with electronic devices and the Internet. This culture, as confirmed by (Al-huwaimel, 2020; Mohammed, 2019) is represented in the protection of personal information, the preservation of the user name and password, protection from fraud, identity theft, and impersonation, protection from bullying and personal harassment via the Internet, getting rid of Internet addiction and social isolation, and dealing well with informational content on the Internet.

2.3.2 Digital Technology Security Culture: It is related to the physical protection of electronic devices and data, which is related to technical procedures in the user's interaction with the computer and the Internet. Valentine et al. (2016) identified this culture in protecting devices from viruses and malware, safe use of the Internet, and data backup.

2.3.3 Social Information Security Culture: It is related to the impact of electronic devices and the Internet on society, and the user's relationship with the surrounding society. It was identified awareness of the potential dangers of using social networking sites on society, protection from groups that advocate extremism and violence, commitment to social and ethical digital behavior, and respect for the intellectual property rights of others. (Mohammed, 2019; Whitmer et al., 2012).

2.4 Secondary Education Role in Enhancing Information Security Culture among Students:

The issue of enhancing information security culture among adolescents and youth has received the attention of many researchers and studies due to the sensitivity of this age stage, and the rapidity of their vulnerability to ideas and information spread on websites. It was indicated that students in the secondary stage go through adolescence and are exposed to some psychological problems. Thus, their social relations with family members and school friends are disrupted. It raises the students' ethics in dealing with networks and websites, and protects them from the risks associated with using the Internet (Al-Saif, 2014).

Although twenty-first-century students are more proficient in using technology than their parents or teachers, it was emphasized that they will always need guidance on how to best use these powerful tools in innovative learning tasks (Trilling & Fadel , 2009). Beuran et al. (2016) confirmed that it is important that information security education not only be applied by people who work in the field of information technology, but should include ordinary people who represent the vast majority of Internet users.

Martin et al. (2018) demonstrated that cyberbullying, digital identity, digital printing, and inappropriate social media use are topics of

interest in general education schools. With the increasing number of schools and school districts implementing initiatives related to bringing student electronic devices to school, the importance of teaching these subjects in schools increased.

Al-Arishi & Aldossary (2018) indicated that it is necessary for schools to inculcate the basics of information security and safety in the minds of students, especially in light of the electronic attack on data and websites that the world is facing. This can be through educating students about the importance of the data and information being circulated and preserving it from theft or leakage.

Hence, schools' responsibility towards educating students and protecting them from the risks and threats they face has increased, especially those related to the cultural and informational aspects that have become the dominant feature of this era. They also protect them from the consequent crimes or moral deviations they may be exposed to while dealing with technological applications.

Ribble (2015) has sought to devise an educational model to help students start thinking about how to use technology in schools and at home appropriately taking into consideration that they live in a world saturated with digital technology. The model includes four phases as follows:

- **Awareness and Perception Phase:** It focuses on helping students become technically literate. This stage goes beyond basic knowledge of computer parts and programs and knowledge of the appropriate use of these digital technologies.

- **Guided Practice Phase:** After following the instructions in the awareness phase, teachers train students to practice the appropriate use of digital technologies, so that students are given an opportunity to learn these principles in an environment that encourages discovery.

- **Acting and Presentation Phase:** Teachers provide students with explicit acting lessons that focus on appropriate use of technology in the classroom, so that teachers practice good digital usage habits in front of the students.

- **Feedback and Analysis Phase:** Technology use inside and outside the school is evaluated through classroom activities in which students participate, to ensure that students use technology effectively and appropriately.

3. METHODOLOGY:

3.1. Study Methodology: The descriptive method was used in the current study. A questionnaire was administered to collect data about secondary education's role in enhancing information security culture, its obstacles, and requirements for activation.

3.2. Study Population: The study population consists of all teachers and students in secondary schools in Saudi Arabia.

3.3. Study Sample: A stratified random sample of (267) male and female teachers in secondary schools in Saudi Arabia was selected and distributed to the study variables as shown in the following table:

Table (1) Study Sample Percentage

Variable	Description	Participants	Percentage
Gender	Male	148	55.4 %
	Female	119	44.6 %
Years of Experience	Less than 5 years	36	13.5 %
	5 years to less than 10 years	70	26.2 %
	10 years and more	161	60.3 %

Total	267	100 %

3.4. Questionnaire Design: The study used a questionnaire consisting of two parts. The first part is about general information. The second part consists of three pivots: the first one is to identify the secondary education role reality in enhancing information security culture among students, consisting of (13) statements; the second one is to identify the obstacles to enhancing information security culture among students, consisting of (7) statements; and the third pivot is to identify the requirements for activating the role of secondary education in enhancing information security culture among students, consisting of (8) statements. The five-point Likert scale was used (5 very large agree, 4 Large agree, 3 moderately agree, 2 Weak agree, 1 very Weak agree) to answer the questionnaire.

3.5. Validity: The validity of the questionnaire was verified by (11) experts, to know their opinions on its dimensions, pivots, and statements, and the extent to which the statements are related to its dimensions. It was modified in light of their opinions. The internal consistency was also verified by calculating Pearson coefficient between the statement's score and the total score given to the dimension under which this statement was categorized. The correlation coefficients ranged as follows: the dimension of the secondary education role reality in enhancing information security culture among students from (0.80 - 0.96), and the dimension of the obstacles to enhancing information security culture among students from (0.80 - 0.91), and the last dimension of requirements for activating the role of secondary education in enhancing information security culture among students from (0.73 - 0.87).

3.6. Reliability: The reliability of the questionnaire as a whole and its dimensions was verified by calculating Cronbach's alpha coefficient. The reliability coefficient for the secondary education role reality in enhancing information security culture among students was (0.98), the obstacles to enhancing information

security culture among students was (0.95), and the requirements for activating the role of secondary education in enhancing information security culture among students were (0.91), and the questionnaire as a whole was (0.86).

3.7. Study Procedures: A questionnaire was prepared and verified for its validity, reliability, and suitability for implementation. It was administered electronically to teachers in secondary schools in Saudi Arabia.

3.8. Statistical Procedures: The SPSS 24 program was used to calculate the Pearson correlation coefficient to verify the validity of the questionnaire, Cronbach's alpha coefficient to verify the stability of the questionnaire, the calculation of the arithmetic mean (M) and the standard deviation (SD) of the dimensions and statements of the questionnaire, the calculation of the t-test, and the ANOVA test to find out the differences between the study variables, as well as the Scheffe's test to determine the differences between more than two variables.

The weight value of the responses was calculated in order to identify the degree of agreement of the sample participants to the statements and dimensions of the questionnaire. Thus, if the response was (very Weak) in the dimension or statement when the arithmetic means was (1.79) or less, it was (Weak) when the arithmetic means were limited from (1.80) to (2.59), it was (moderately agree) when the arithmetic average was limited from (2.60) to (3.39), (large agree) when the arithmetic average was limited from (3.40) to (4.19), and (very large agree) when the arithmetic average was (4.20) or more.

4. Results:

4.1 Results of the Secondary Education Role Reality in Enhancing Information Security Culture among Students:

Table (2) Arithmetic Mean and the Standard Deviation of Secondary Education Role Reality in
Enhancing Information Security Culture among Students

No.	Phrases	M	S.D	Rank
1	The school organizes training courses to educate students about information security culture.	2.19	0.94	11
2	The school allocates an open day to present the concepts and risks of information security to students.	2.01	1.08	13
3	The school is concerned with educating students about the standards and controls for safe use of the Internet.	2.43	1.28	2
4	The school demonstrates the elements of information security: confidentiality, integrity, and availability to students.	2.26	1.25	9
5	The school educates students not to disclose personal data on the Internet.	2.50	1.31	1
6	The school urges students to avoid communication with unknown people via social networks.	2.42	1.37	3
7	The school urges students to choose strong passwords for personal accounts.	2.37	1.29	6
8	The school encourages students to ignore anonymous online offers and applications.	2.42	1.27	3
9	The school educates students about the dangers of cybercrime and the leniency in protecting important information.	2.42	1.29	3
10	The school trains students on how to obtain reliable sources of information.	2.13	1.32	12
11	The school explains to students the positive aspects of information security culture on individuals and society.	2.24	1.33	10
12	The school shows students ways to protect against malicious software.	2.27	1.37	8
13	The school encourages students to report information breaches.	2.29	1.39	7
The reality of enhancing information security culture as a whole		**2.31**	**1.16**	

It is clear from table (2) that the arithmetic mean of the secondary education role reality in enhancing information security culture dimension was (2.31), the standard deviation was (1.16), and the degree of agreement was weak. The arithmetic mean of the statements was limited between (2.01-250), and the degree of agreement to the statements was weak. The standard deviation ranged from (0.94 - 1.37) , This result confirms the presence of convergence in the opinions of the study sample. The two statements (5 & 3): "*The school educates students not to disclose personal data on the Internet*" and "*The school is concerned with educating students*

about the standards and controls for safe use of the Internet" were with the highest arithmetic mean: (2.50, 2.43) respectively. They were in the first and second ranks. Other two statements (10 & 2): "*The school trains students on how to obtain reliable sources of information*" and " *The school allocates an open day to present the concepts and risks of information security to* *students*" were with the lowest arithmetic mean (2.13, 2.01). They were in the last two ranks.

4.2 Results of Obstacles to Enhancing Information Security Culture among students in secondary education :

Table (3) Arithmetic Mean and the Standard Deviation of Obstacles to Enhancing Information Security Culture

No.	Phrase	M	S.D	Rank
1	The school administration's lack of interest in the availability of training courses to provide students with information security culture.	3.84	1.16	7
2	Not allocating an adequate budget to implement plans and programs related to information security in schools.	3.99	1.23	6
3	Not including information security topics within the content of academic courses.	4.14	1.06	2
4	Poor students' practice of information security activities and programs within the academic plan.	4.03	1.09	5
5	Lack of teachers specialized in the information security field in schools.	4.09	1.15	3
6	Lack of activities dedicated to spreading the information security culture in schools.	4.13	1.11	4
7	Lack of equipment, devices, and technology necessary to implement information security activities in schools.	4.47	0.75	1
Obstacles to enhancing information security culture as a whole		4.09	0.89	

It is clear from table (3) that the arithmetic mean of the obstacles to enhancing information security culture dimension was (4.09), the standard deviation was (0.89), and the degree of agreement to the dimension as a whole was high. The arithmetic mean of the statements was limited between (3.84- 4.47). The degree of agreement to the statements ranged from (large agree- very large agree). The standard deviation of statements ranged from (0.75 - 1.23). This result confirms the presence of convergence in the opinions of the study sample. The two statements (7 & 3), "*Lack of equipment, devices, and technology necessary to implement* *information security activities in schools*" and "*Not including information security topics within the content of academic courses*" were with the highest arithmetic mean: (4.47, 4.14) respectively, They were in the first and second ranks. Other two statements (2 & 1),"*Not allocating an adequate budget to implement plans and programs related to information security in schools*" and "*The school administration's lack of interest in the availability of training courses to provide students with information security culture*" were with the lowest arithmetic mean (3.84, 3.99).They were in the last two ranks.

4.3 Results of Requirements for Activating secondary education Role in Enhancing **Information Security Culture:**

Table (4) Arithmetic Mean and the Standard Deviation of Requirements for Activating secondary education Role in Enhancing Information Security Culture

No.	Statement	M	S.D	Rank
1	The school administration conviction of the importance of students' practice of information security activities and programs.	3.94	1.10	7
2	Issuing laws and legislations to teach information security to students in schools.	3.91	1.21	8
3	Holding training courses to provide students with safe methods for dealing with modern technologies.	3.99	1.26	4
4	Develop comprehensive plans to practice information security activities and programs within the school's academic plan.	3.98	1.25	5
5	Developing course content and including information security topics.	4.05	1.15	3
6	Providing an independent budget for the implementation of information security activities and programs in schools.	3.97	1.20	6
7	Providing modern devices and technology necessary to implement information security activities in schools.	4.39	0.99	1
8	Holding interactive dialogues with students about information security.	4.16	1.16	2
Requirements for activating information security culture as a whole		**4.07**	**0.84**	

It is clear from table (4) that the arithmetic mean of the requirements for activating the secondary education role in enhancing information security culture dimension was (4.07), the standard deviation was (0.84), and the degree of agreement to the dimension as a whole was high. The arithmetic mean of the statements was limited between (4.39 - 3.91). The degree of agreement to all requirements was high. The standard deviation ranged from (0.99 - 1.26). This result confirms the presence of convergence in the opinions of the study sample. The two statements (7&8): "*Providing modern devices and technology necessary to implement information security activities in schools*" and "*Holding training courses to provide students with safe methods for dealing with modern*

technologies" were with the highest arithmetic mean: (4.39, 4.16) respectively, They were in the first and second ranks. The other two statements (1 & 2): "*The school administration conviction of the importance of students' practice of information security activities and programs*" and "*Issuing laws and legislations to teach information security to students in schools*" were with the lowest arithmetic mean (3.94, 3.91). They were in the last two ranks.

4.4 Results of Differences among Study Sample Mean Scores in the Secondary Education Role Reality in Enhancing Information Security Culture, Obstacles, and

Requirements for Activation According to Gender and Years of Experience :

4.4.1 Results of Differences among Study Sample Mean Scores in the Secondary Education Role Reality in Enhancing Information Security Culture, Obstacles, and Requirements for Activation According to Gender:

Table (5) T-test Results between Males and Females teacher in Secondary Education Role Reality in Enhancing Information Security Culture, Obstacles, and Requirements for Activation

Dimension	Gender	N	M	SD	Df	T	Sig.
Secondary Education Role Reality in Enhancing Information Security Culture	Male	148	2.18	1.17	265	1.98	0.049
	Female	119	2.46	1.13			
Obstacles to Enhancing Information Security Culture	Male	148	3.99	0.94	265	2.06	0.045
	Female	119	4.22	0.83			
Requirements for Activating Information Security Culture	Male	148	4.25	0.74	265	3.89	0.000
	Female	119	3.86	0.89			

It is clear from table (5) that there are statistically significant differences at the significance level ($\alpha \leq 0.05$) between males and females in the secondary education role reality in enhancing information security culture among students and its obstacles in favor of females. There are also statistically significant differences at the significance level ($\alpha \leq 0.001$) between males and females in requirements for activating information security culture in favor of males.

4.4.2 Differences among Study Sample Mean Scores in the Secondary Education Role Reality in Enhancing Information Security Culture, Obstacles, and Requirements for Activation According to Years of Experience:

Table (6) ANOVA Test among Study Sample Mean Scores in Secondary Education Role Reality in Enhancing Information Security Culture, Obstacles, and Requirements for Activation according to Years of Experience

Dimension		Sum of Squares	df	Mean Square	F	Sig
The reality of Enhancing Information Security Culture	Between Groups	40.443	2	20.222	16.768	0.000
	Within Groups	318.384	264	1.206		
	Total	358.827	266			
Obstacles to Enhancing Information Security Culture	Between Groups	4.500	2	2.250	2.817	0.062
	Within Groups	210.854	264	.799		
	Total	215.354	266			

Requirements for Activating Information Security Culture	Between Groups	12.835	2	6.417	9.772	0.000
	Within Groups	173.367	264	.657		
	Total	186.201	266			

It is clear from table (6) that there are no statistically significant differences among teachers in the obstacles to enhancing information security culture according to years of experience. However, there are statistically significant differences at the significance level ($\alpha \leq 0.001$) among teachers in the reality of enhancing information security culture and its activation requirements according to years of experience. Due to the results of Scheffe's test, those differences will be found in the reality of enhancing information security culture pivot among teachers with an experience less than (5) years, teachers with an experience from (5) years to less than (10) years, and teachers with an experience more than (10) years in favor of teachers with an experience less than (5) years. However, there is no statistically significant difference among teachers with an experience more than (10) years, and teachers with an experience from (5) years to less than (10) years. According to Scheffe's test results, there are statistically significant differences among teachers with an experience less than (5) years, teachers with an experience from (5) years to less than (10) years, and teachers with an experience more than (10) years in the requirements for activating the secondary education role in enhancing information security culture among students in favor of teachers with an experience from (5) years to less than (10) years. Furthermore, there are no statistically significant differences among teachers with an experience less than (5) years and those with an experience of more than (10) years.

5. Discussion Results :

5.1. The Secondary Education Role realty in Enhancing Information Security Culture among Students:

The results showed the weak role of secondary education in enhancing information security culture among students (M= 2.31). Due to these results, it is found that they are compatible and consistent with reality, as secondary schools focus on teaching the content of academic courses only without paying attention to activities that enhance information security culture among students. Moreover, secondary schools are not concerned with holding training courses to educate students about the information security culture to identify the standards and controls for safe use of the Internet, the danger of disclosing personal data on the Internet or communicating with anonymous people through social networks, and how to obtain reliable sources of information. There is also a lack in the secondary schools' interest in providing students with the dangers of information crimes on individuals and society, methods of protection from malicious programs and reporting electronic violations.

This result is consistent with the findings of a number of studies that emphasized the weak role of secondary schools in promoting behaviors related to information security among students (Al-Zahrani et al., 2020; Al-Manea, 2015; Sayed, 2015).This result is also consistent with the findings of the study carried out by Gharib & Al-Amir (2017), which confirmed the low awareness of secondary school students about information security, and that (57%) of students do not set a password to protect their personal computers, and (41%) do not change passwords continuously.

5.2. Obstacles to Enhancing Information Security Culture among Students:

The results showed that there are significant obstacles that hinder the secondary school from playing its role in enhancing information security culture among students (M=4.09). This is consistent with the reality as secondary schools do not have the equipment, devices and technology necessary to implement information security activities. In addition, there is no

sufficient budget to implement plans and programs related to information security for students, as well as the failure to include information security topics within the content of the academic courses. There is also a lack of teachers specialized in the field of information security and activities dedicated to spreading the culture of information security. This result is consistent with the findings of El-Sayed (2017), which confirmed the presence of many difficulties that hinder high schools in managing information security operations.

5.3. Requirements for Activating secondary education Role in Enhancing Information Security Culture among students:

The results showed the agreement of the study sample to a large extent on the need to provide the necessary requirements to activate the role of secondary schools in enhancing information security culture among students (M=4.07).Moreover, enhancing information security culture requires the following : the school administration's conviction of the importance of students' practice regarding information security activities and programs, the issuance of laws and legislations to teach information security to students in schools, holding training courses to provide students with safe methods to deal with modern technologies, and developing integrated plans to practice information security activities and programs within the academic plans. It is also important to develop the content of the academic courses including topics about information security, provide an independent budget for the implementation of information security activities and programs in schools, as well as holding interactive dialogues with students on information security, This result is consistent with the findings of Al-Obeid (2019), which emphasized the need to provide students with the necessary requirements and teachers with information security culture in secondary schools.

5.4 Mean Differences between Teachers' Responses according to Gender and Years of Experience:

5.4.1 The Gender: Results showed that there are statistically significant differences at the significance level ($\alpha \leq 0.05$) between males and females in the secondary education role reality in enhancing information security culture among students and its obstacles in favor of females. This is due to the increase sense of females regarding the weak role played by the school in enhancing cyber security culture to protect students from electronic dangers, as well as the increased conviction of females that there are significant obstacles in schools that limit their role in providing students with information and cyber security skills. According to females, the school protects students from cyber risks that they may be exposed to, and it must correct the mistakes of other institutions. Results also showed that there are statistically significant differences at the significance level ($\alpha \leq 0.001$) between males and females in requirements for activating information security culture in favor of males. This is due to the males' conviction, more than females, of the importance of providing the necessary requirements to activate the role of secondary schools in enhancing information security culture among students.

5.4.2 Years of Experience : Results showed that there are no statistically significant differences among teachers in the obstacles to enhancing information security culture according to years of experience. This is due to the feeling of all teachers, regardless of the years of experience, that there are significant obstacles that limit the role of secondary schools in enhancing information security culture for their students. In addition, results showed that there are statistically significant differences at the significance level ($\alpha \leq 0.001$) among teachers in the reality of enhancing information security culture according to years of experience in favor of teachers with an experience less than (5) years. This is due to the fact that teachers with less than (5) years of experience have digital and technological skills that enable them to judge the reality of the school's role in enhancing students' information security, and they are more familiar

with digital technology and its risks than others. This result is consistent with the findings of the study investigated by Faraj (2022), which confirmed the existence of differences in favor of teachers with less than (5) years of experience. There are statistically significant differences at the significance level (α≤0.001) among teachers in the requirements of activating information security culture according to years of experience in favor of teachers with an experience from (5) years to less than (10) years. This result is due to the increased conviction of intermediate-experienced teachers more than others of the importance of the Ministry of Education to provide the necessary requirements to activate the role of secondary schools to provide students with information security culture and to familiarize them with the standards and controls for safe use of the Internet.

6. Conclusion:

The study concluded that the role of secondary education in enhancing information security culture among students is weak (M = 2.31), and that there are significant obstacles that limit the role of secondary education in enhancing information security culture among students (M = 4.09).It also found out that the necessary requirements must be provided to activate the role of secondary education in enhancing information security culture among students significantly (M = 4.07).In addition, there are statistically significant differences at the significance level (α≤0.05) between males and females in the secondary education role reality in enhancing information security culture among students and its obstacles in favor of females. There are statistically significant differences at the significance level (α≤0.001) between males and females in requirements for activating information security culture in favor of males. Moreover, there are statistically significant differences at the significance level (α≤0.001) among teachers in the reality of enhancing information security culture according to years of experience in favor of teachers with an experience less than (5) years. There are statistically significant differences at the significance level (α≤0.001) among teachers in

the requirements of activating information security culture according to years of experience in favor of teachers with an experience from (5) years to less than (10) years. However, there are no statistically significant differences among teachers in the obstacles to enhancing information security culture according to years of experience.

7. Recommendations:

In light of the study results, the study recommends that the Saudi Ministry of Education should: issue laws to teach information security in schools, include information security topics in the academic courses, set an independent budget, and provide the modern devices and technology necessary to students to acquire information security culture.

The study also recommends: developing plans and programs to implement information security activities and programs for students in schools, holding training courses and interactive dialogues to provide students with safe methods for dealing with the Internet, and coordinating with the competent cyber security authorities in Saudi Arabia to implement awareness programs for students about information security in schools.

8. References:

[1] Al-Arishi, G & Aldossary, S. (2018). The role of higher education institutions in enhancing information security culture in society. *King Fahd National Library Journal, 24* (2). 302-373.

[2] Al-huwaimel, S. (2020). The effect of the adaptation based on student learning style in improving the digital security skills for third-grade intermediate students. *International Journal of Educational and Psychological Sciences*, *36*(54), 13-106.

[3] Al-Manea, O. (2015). The roles of computer teachers in promoting computer ethics and related educational behaviors in the secondary stage from the point of view of educational supervisors. *Studies - Educational Sciences, 43*(3), 1891-1907.

[4]   Al-Montashari, F. (2019). *Awareness of middle school teachers in public schools in Jeddah about cybersecurity*. Master's Thesis, Dar Al-Hekma University, Faculty of Health and Behavioral Sciences and Education.

[5]   Al-Obaid, M.(2019). Information security demands in computer textbooks in adult secondary schools. *International Journal of Specialized Qualitative Research, 20*, 13-31

[6]   Al-Rabiah, S. (2017). *Digital security and user protection from the dangers of the Internet,* Riyadh: Communications and Information Technology Commission.

[7]   Al-Saif, A. (2014). A proposed program in Internet culture to develop an awareness of some life issues in the intermediate and secondary stages, *Journal of Educational Sciences, 26* (1), 19-45.

[8]   Al-Zahrani, J., Eidi, S., Al-Ghamdi, J., Al Yafei, B., Al-Qaidi, A.& Bawazir, W. (2020).The degree to which secondary school students in Jeddah governorate practice the concept of digital security and digital rights and responsibilities. *International Journal of Educational and Psychological Sciences, 40*, 356-390.

[9]   Beuran, R., Chinen, K., Tan, Y.& Shinoda, Y.(2016). *Towards Effective Cybersecurity Education and Training*, https://www.jaist.ac.jp/~razvan/publications/effective_cybersecurity.pdf

[10] Chang, X., Pei, S. & Su, Na .(2013). Research on Real-Time Network Forensics Based on Improved Data Mining Algorithm. *Applied Mechanics and Materials , 380-384*, 1881-1885, https://doi.org/10.4028/www.scientific.net/AMM.380-384.1881 ,

[11] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4* (10), 13–21. http://timreview.ca/article/835

[12] Elsayed, W. (2017). A Suggested strategy for information security processes management at industrial secondary education schools in A. R.E.. *Educational Administration Journal*, (12) , 401-560

[13] Faraj , A . (2022).The reasons for promoting Cyber Security Culture in Light pf digital transformation prince sattam Bin Abdulaziz University as a Model. *Educational Journal, 1*(94), 510-537.

[14] Gharib, M. & Al-Amir, H. (2017). The extent of awareness among the young age group of the Saudi cybercrime penal system. *International Journal of Informatics, 5*(9), 7-32.

[15] Goran, I.(2017). *Cyber Security Risks in Public High Schools*, master thesis, John Jay College of Criminal Justice- City University of New York, https://academicworks.cuny.edu/jj_etds/5/

[16] Martin, F.& Whitmer, J.(2016). Applying Learning Analytics to Investigate Timed Release in Online Learning. *Technology, Knowledge and Learning*, (21), 59–74 , https://link.springer.com/article/10.1007/s10758-015-9261-9

[17] Martin, F., Wang, C., Petty, T. , Wang, W.& Wilkins, P.(2018). Middle school students Social Media Use. *Journal of Educational Technology & Society , 21*(1), 213-224, https://www.jstor.org/stable/26273881

[18] Mohammed, N. (2019). Interaction between the patterns of Gamification (points/leaderboard) and Learning Style (Ambiguity / Non-ambiguity) and Its Effect on Developing Digital Security Skills and Self-Directed Learning among Umm Al-Qura University students. *Journal of Faculty of Education, 30* (120), 495-573.

[19] Rahman, N., Sairii, I., Zizi ,N. & Khalid F.(2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, 10* (5), http://www.ijiet.org/vol10/1393-JR419.pdf

[20] Ribble, M.(2015). *Digital Citizenship in Schools: Nine Elements All Students Should Know* (3rd ed). International society for technology in Education.

[21] Saegh, W. (2018). Awareness of family members with the concept of cybersecurity and its relationship to their security

precautions against cybercrime. *The Arab Journal of Social Sciences, 14*(3). 18-70.

[22] Sayed, R. (2015). Electronic book crimes: An analytical study to develop a protection strategy for them, *King Fahd National Library Journal, 21* (2), 209-298.

[23] Solms, R. & Solms, S. (2015). Cyber safety education in developing countries, Systemics , *Cybernetics and Informatics. 13* (2), 14-19, http://hdl.handle.net/10204/8315

[24] Trilling, B.& Fadel, C. (2009). *21st Century Skills: Learning for Life in Our Times*. New York: John Wiley & Sons

[25] Valentine, S., Leyva-McMurtry, A., Borgos-Rodriguez, K. & Hammond, T. (2016). The Digital Sash: A Sketch-Based Badge System in a Social Network for Children. in *Revolutionizing Education with Digital Ink* , 179–189, Hammond,T. , Valenline, S. & Adler,A. (ed), New York ; Springer International Publishing, https://link.springer.com/book/10.1007/978-3-319-31193-7

[26] Whitman, M. & Mattord, H.(2017). *Principles of Information Security* (6th Ed), Bosten: Cengage Learning.

[27] Whitmer, J., Fernandes, K. & Allen, W. (2012). *Analytics in Progress: Technology Use, Student Characteristics, and Student Achievement*, https://er.educause.edu/articles/2012/8/analytics-in-progress-technology-use-student-characteristics-and-student-achievement.

[28] Wilson, C . (2014). Cybersecurity Education: The Emergence of an Accredited Academic Discipline?. *Journal of The Colloquium for Information Systems Security Education (CISSE)*. 2 (1), 1-13, https://cisse.info/journal/index.php/cisse/article/view/14/CISSE_v02_i01_a06.pdf,

[29] Yilmaz , R., Karaoglan, F., Özturk, H. & Karademir, T. (2017). Examining Secondary School Students' Safe Computer and Internet Usage Awareness: An Example from Bartin Province. *Pegem Eğitim ve Öğretim Dergisi*, *7* (1), 83-114. https://files.eric.ed.gov/fulltext/ED572474.pdf

[30] Zaghloul, B. & Shehata, H. (2019). A proposed digital unit to develop information security awareness among commercial secondary school students. *Journal of the Faculty of Education, 7* (31), 889-904.