Migration Letters

Volume: 20, No: 6, pp. 1111-1128

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

The Impact of Digital Education on Acquiring Cybersecurity Skills among the Students of the Faculty of Medicine at Al-Balqa Applied University

Barween Al Kurdi[1], Mohamad Ali Al Anasweh[2], Haitham M. Alzoubi[3], Areeg Al Fouri[4], Dr. Shatha Sakher[5], Muhammad Turki Alshurideh[6]

Abstract

The study aimed to identify the impact of digital education (digital citizenship, digital skills, digital culture) on acquiring cybersecurity skills (the concept of cybersecurity, cybercrime, cybersecurity challenges). It also aimed to identify both the level of digital education and the level of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University. The researcher used the descriptive analytical approach through the study tool, i.e. the questionnaire. The study sample consisted of (150) students withdrawn from the study population through random sampling. The results showed that the level of digital education among the students of the Faculty of Medicine at Al-Balqa Applied University was moderate. The level of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University was also moderate. Moreover, the results indicated a statistically significant effect of digital education in all its dimensions (Digital citizenship, digital skills, digital culture) on acquiring cybersecurity skills in its combined dimensions (the concept of cybersecurity, cybercrime, cybersecurity challenges) at a significant level ($\alpha \leq 0.05$) among students of the Faculty of Medicine at Al-Balqa Applied University. The study recommended a number of recommendations, including enhancing the acquisition of cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University through a contract to raise and increase the understanding of the concept of cybersecurity and increasing the courses offered to them in the field of digital laws and various digital skills.

Keywords: *digital education, acquiring cybersecurity skills.*

1. Introduction

Communication networks are an ideal medium for the flow of data. In recent years, organizations have relied heavily on information technology in their business, which requires protection and the safety of this technology and electronic networks from several risks to ensure business continuity and not to be hacked, stolen, destroyed, or exposed to

[1] Department of Marketing, Faculty of Business, The Hashemite University, P.O. Box 330127, Zarqa 13133, Jordan. https://orcid.org/0000-0002-0825-4617 , Email: barween@hu.edu.jo

[2] Associate Professor, Al-Balqa Applied University, Department of Library and Information Management, abothamer12345@bau.edu.jo

[3] a. School of Business, Skyline University College, Sharjah, UAE. haitham_zubi@yahoo.com,b. Applied Science Research Center, Applied Science Private University, Amman, Jordan. [0000-0003-3178-4007].

[4] Head of the Scientific Research Division, Faculty of Medicine, Al-Balqa Applied University, As-Salt, Jordan. areeg.alfouri@bau.edu.jo

[5] Faculty of Medicine, Al-Balqa Applied University, As-Salt, Jordan, Shatha.sakher@bau.edu.jo, shatha.s.zoubi@gmail.com, https://orcid.org/0000-0001-6555-9911

[6] Department of Marketing, School of Business, The University of Jordan, Amman 11942, Jordan, https://orcid.org/0000-0002-7336-381X, m.alshurideh@ju.edu.jo

viruses and malware. Therefore, many organizations set out to prepare a comprehensive strategy to ensure information security in cyberspace since cybersecurity relies on a wide range of legal and technical methods to confront the illegal use of the Internet and various means of communication. This is done by building firewalls to prevent electronic attacks and reduce breaching, spying, and theft of government and private accounts and information systems (Waliyuddin & Sulisworo, 2022).

The completion of this step requires obtaining the best technological means and methods, with the need to spread awareness of the importance of cybersecurity and ways to maintain the informational structure of the various systems, especially for the various means of communication, whether official or private, in addition to the training, education and awareness processes. Thus, it was necessary to direct the individuals' culture towards digital education, which aims to enhance cyber protection and security and protect individuals from hacking. These may be used to steal financial or personal information, exposing individuals to the blackmailing process (Al-Sawat and Al-Mana'a, 2020).

Educational institutions play a vital role in promoting the concept of cybersecurity whose knowledge contributes to the identification of educational methods and means. These include preserving society's core values, such as belonging, beliefs, customs and traditions, and avoiding the risks faced by information systems and devices connected to the Internet, such as mobile phones and PCs (Cham et al., 2021).

2. Research problem

As a result of the changes in the nature and methods of communication, which shifted from traditional to technological methods, especially for the emerging generation and students, educational institutions must prepare programs related to preserving cybersecurity and educating students about its skills. This is known as digital education, mainly based on setting controls that make generations use technology within a scope that does not negatively affect their real lives, such as violating intellectual property rights, violating privacy, providing a fertile environment for any kind of prohibited trade, and money laundering (Al-Manthari, 2020). Due to the importance of cybersecurity, the world tends to make widespread and extensive use of artificial intelligence and totally rely on computer technologies and programs, and the density of information stored in computer systems, which requires increasing the security and protection of networks, reducing electronic piracy, and protecting data and websites from violations, theft, and breaching.

In this context, the importance of digital education comes from spreading cyberspace's security culture. This study answers the main question: What is the impact of digital education on acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University?

In light of the main question, a number of sub-questions were branched out as follows:

- What is the relative importance of digital education among students of the Faculty of Medicine at Al-Balqa Applied University?

- What is the relative importance of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University?

3. Objectives of the study

This study aims to:

- Identify the impact of digital education (digital citizenship, digital skills, digital culture) on acquiring cybersecurity skills (the concept of cybersecurity, cybercrime, cybersecurity

challenges) among students of the Faculty of Medicine at Al-Balqa Applied University. Several sub-objectives derive from this objective:

- Identifying the level of digital education among students of the Faculty of Medicine at Al-Balqa Applied University.
- Identifying the level of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University.

4. Significance of the study

The importance of the present study stems from its focus on the level of digital education and its impact on the acquisition of cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University.

- Scientific significance:

This study is expected to interest most researchers, analysts, and those interested in the subject of the study. Digital education and its impact on the acquisition of cybersecurity skills are addressed. Therefore, this study presents new results showing the importance of digital education and its elements and offers appropriate recommendations. Therefore, we hope this study will be significant for researchers and those interested in the subject of the study and to gain new results related to the topic.

- Practical significance:

The practical significance of this study is to know the impact of digital education in its dimensions (digital citizenship, digital skills, digital culture) in acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University. This has an impact on the social and security dimensions. It also affects students' scientific values. It is expected that the results of the study will be of interest in digital education, acquiring cybersecurity skills, and providing Arab libraries with such topics

5. The hypothesis of the study

This study sought to test the following hypothesis:

Ho1: digital education with its dimensions (digital citizenship, digital skills, digital culture) has no statistically significant effect on the acquisition of cybersecurity skills (the concept of cybersecurity, cybercrime, cybersecurity challenges) among the students of the Faculty of Medicine at Al Balqa Applied University.

6. Procedural definitions

Digital Education is described as a set of customs, traditions, values, skills, knowledge, and codes of conduct related to dealing with technology and various digital devices to constitute a positive tool to achieve the tasks that individuals practice practically, scientifically, and socially (Naziha and Manoubia, 2021). Also, it is defined procedurally as a set of customs, traditions, norms, principles, and ideas that students learn in their educational and social environment. They are applied and practiced while dealing with technological tools and social media applications. To add more, Cybersecurity is related to information on devices and internet networks and processes by which equipment, services, and information are protected from any unauthorized or intended interference, change, or difference that may occur. Hence, several organizational, technical, and administrative methods are used to prevent unauthorized use and abuse (Al-Mantashari, 2020).

It is procedurally defined as the security of student's personal information on their electronic accounts, mobile phone, and electronic devices that protect them from hacking and theft and enable them to preserve their privacy.

7. The limits and determinants of the study

The limits of this study are as follows:

- Spatial limits: Faculty of Medicine, Al Balqa Applied University.

- Temporal limits: the period between (2022-2023).

- Human Limits: Students of the Faculty of Medicine at Al-Balqa Applied University.

- Thematic limits: Knowing the impact of digital education on the acquisition of cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University.

8. Literature Review

The most significant literature, from the most recent to the oldest investigations, is listed here. The following sections are how they are presented: From the perspective of teachers at a rehabilitation center for the blind in Biskra City, Naziha and Manoubia (2021) sought to understand the reality of smart digital education in rehabilitation programs for persons with special needs. In order to describe the reality of smart digital education in the qualifying programs for this category and to pinpoint the key difficulties in utilizing contemporary technology to teach and certify this group, the descriptive approach was adopted. The findings of this study suggest that conventional approaches are used to teach and rehabilitate the blind instead of using any current technologies. This indicates the government's lack of interest inThere is a statistically significant positive correlation between the early childhood teacher's possession of digital education and possession of twenty-first-century skills at a significance level of (0.01). The study recommended holding training courses and workshops for teachers, especially beginners, to help them acquire the necessary skills for the twenty-first century. It also recommended empowering female teachers to prepare and design educational software for the new curriculum. Further, Faculty should prepare early childhood teachers by integrating and including twenty-first-century skills in their programs. To add more, Al-Manthari (2020) examined the role of school administration in enhancing cyber security in government schools for girls in Jeddah from the point of view of female teachers, presenting a proposed vision for the role of school management in enhancing cyber security in government schools for girls in Jeddah. The study followed the descriptive analytical approach. A questionnaire consisting of two axes was prepared: the role of school leadership in enhancing cybersecurity for female teachers and the role of school leadership in enhancing cybersecurity for school students. It was applied to a sample of 420 female teachers in a number of government schools in Jeddah. The study results showed that the role of school leadership in enhancing cyber security for female teachers and female students is achieved with a low degree of approval from the female teacher's point of view. In light of these results, the study proposed a vision for the role of school leadership in enhancing cyber security for female teachers and students. It was implemented in coordination with the competent authorities concerned with cybersecurity in Saudi Arabia. It included mechanisms for female teachers, female students, female teachers and female students together, in addition to mechanisms for protecting the physical environment of the Internet.

Alsawat and Almanaa (2020) investigated how much cybersecurity knowledge there was among primary and intermediate school pupils in Taif and how it related to the presence of civic, moral, and religious values. In order to demonstrate the predictability of these values

through knowledge of cyber security, they also examined the relationship between awareness of cyber security and their values. Finally, the researchers looked at how the variables (gender, kind of school, level of schooling, and economic condition of the family) affected the respondents in the study sample in terms of cybersecurity awareness and values. 346) students made up the study sample. The findings demonstrated that Taif pupils in the primary and intermediate grades are well aware of cybersecurity issues and safe Internet browsing practices.

Through an integrated testing tool with augmented reality (AR) and Google Scholar (GS), Waliyuddin & Sulisworo (2022) attempted to develop assessment tools in the student learning process in an interactive way to improve students' higher-order thinking skills. This was done to encourage students' higher-order thinking skills and digital skills. Students in Sulaiman, Indonesia's 11th grade participated in the test experiments. The findings demonstrated that students' higher order thinking skills are enhanced when augmented reality is used successfully and efficiently in the classroom. To help students strengthen their critical thinking abilities, learning media based on augmented reality may be created. To help pupils develop their digital literacy for the twenty-first century, the study suggested incorporating augmented reality technologies into the teaching process. Also in 2021, Cham et al. sought to change graduate students' perspectives on digital technology.

8.1 Definition of digital education

Naziha and Manobia (2021) define digital education as a set of habits, traditions, values, skills, knowledge, and codes of conduct related to ways of dealing with technology and various digital devices to constitute a positive tool to achieve the tasks that individuals practice practically, scientifically, and socially.

The importance of digital education is seen by (Awad and Al-Tohamy, 2020) as a special process for controlling technological and cultural openness. It serves as a tool for filtering good information that does not contradict society’s values and culture. It enables educational institutions to employ technology appropriately and efficiently, which enables them to make the most of their capabilities. It also enables the employees to complete their tasks and activities faster and with less effort. From a social perspective, digital education contributes to the individuals’ knowledge of the cultures and beliefs of countries without prejudice to their own culture and belief. It also enables individuals to keep pace with technology and the successive and rapid scientific developments in this field.

8.2 Dimensions of digital education

8.2. A: Digital citizenship

Khalifa (2022) defines digital citizenship as the set of regulations, rules, standards, ideas, principles, and norms used positively in the processes related to technology tools and what emerges from them. Also, Awad and Al-Tohamy (2020) indicated that digital citizenship aims to find the right ways to guide and protect all users, especially children and adolescents, by encouraging desirable behaviors and confronting unacceptable ones in digital transactions. To add more, according to Nazihah and Manobia (2021), digital citizenship is the rules followed in the behavior adopted while using technology, such as using it for electronic data exchange, electronic sharing among the various parties in society, and online buying and selling.

8.2.B: Digital skills

Ghavifekr (2022) explains that the most important digital skills are:

1. Basic skills: related to using electronic devices, such as turning devices on and off, installing and managing applications, and logging in to various applications. They also include creating a new user, managing a personal account, joining various electronic

groups, saving and sharing resources and links, and dealing with device accessories, such as audio and video recording devices.

2. Online study skills: Students' ability to access websites appropriate for their academic and practical needs in terms of the required information, the means of keeping and storing it, and their ability to distinguish between correct and incorrect information.

3. Self-learning skills: Individuals' ability to access educational websites that help them improve and develop their knowledge and scientific levels.

4. Problem-solving skills: The ability of individuals to deal with unconventional issues and situations they face and the ways and methods of applying strategies to solve these issues.

5. Crisis management skills: the ability of individuals to understand the nature of situations and issues that occur in an emergency, to deal with them seriously, and the ability to act in these times.

8.2.C: Digital culture:

Awad and El-Tohamy (2020) indicated that digital culture is the awareness of technology, its use, and how it works to benefit from it. They explained that there are several methods for digital culture:

1. Being able to learn about technology before using it.

2. Checking the validity and accuracy of the information and evaluating the various sources on the Internet.

3. Sharing correct information on social media.

4. Developing and detecting patterns of online and distance learning.

5. Recruitment of technology teachers with new and innovative methods to stimulate students' learning and develop their technological skills.

6. Providing accurate digital content related to various educational fields.

8.2.D: Cyber security:

Cyber security is protecting systems, communications, data, and networks connected to the Internet against cyber-attacks and electronic piracy that fall under attempts to hack, disrupt, or illegally log in. Thus, these cyber attacks range from installing malicious codes on devices to attempting to destroy the country's entire infrastructure (Al-Mantashari, 2020). Also, it is the practice associated with protecting systems, networks, and software from any digital attacks to access or destroy sensitive information, extort money from individuals or interrupt commercial operations (Al-Haddad, 2022). Moreover, For individuals, cyber security processes are linked to understanding key data security principles, such as choosing strong passwords, being careful of any attachments received via e-mails or any electronic method from an unknown source, and backing up important data. It also includes ensuring that standard technology used to protect these devices and networks is installed, such as firewalls, DNS filtering, MALWARE, antivirus software, and proposed solutions for e-mail security (Ahmed et al., 2022).

The field of cybersecurity, as seen by (Al-Sawat and Al-Mana, 2020), are explained as follows:

1. Information assurance: measures to protect information to ensure its availability, integrity, and non-violation. It includes providing information systems recovery by integrating protection and detection systems and their ability to interact.

2. Information protection: from any intrusion, disruption, modification, unauthorized access, or illegal exploitation.

3. Information integrity: protecting information from destruction and ensuring that information is credible and not violated.

4. Confidentiality of information: maintaining authorized restrictions on access and disclosure and includes ways to protect personal privacy and property information.

5. Information availability: that is, ensuring reliable and timely access to information and its use when needed.

Types of cybersecurity (Al-Manthari, 2020):

1- Information security: Preserving the integrity of information and privacy during storage and transmission.

2- Application Security: Monitoring and ensuring that programs are free of threats and viruses.

3- Network Security: Securing protection for electronic networks from viruses or hackers.

4- Operation Security and Identity Access and Management: Includes all permissions for network access, storage, and data protection when sharing.

5- Incident recovery and business continuity: aims to restore organizations to their operational capacity as before.

6- User Education: How to deal with any cyber security developments that are difficult to predict.

This study assumes that the dimensions of cybersecurity appropriate for its population include the concept of cybersecurity, cybercrime, and cybersecurity challenges. According to Al-Aqla and Ali (2022), cybercrime is an offence committed against individuals or groups with a criminal motive to offend and defame the victim, physically or mentally, directly or indirectly, through modern means of communication, such as the Internet and e-mail. Also, Al-Haddad (2022) argues that electronic crime tools are diverse. They include software for copying information stored in computers, the Internet as a mediator for the execution of crimes, telephone lines that connect cameras and spy devices, digital coding scanning tools (Barcode), and mobile phones and digital landline phones. In addition, Ahmed et al. (2022) also mentioned a number of destructive software: such as the Trojan software, which is based on deceiving the user to run it as security software but leads to disabling the device; and the worm program, which is similar to a virus but infects the computer without the need for any action and often occurs when an e-mail is sent to all the contacts available in the contacts register.

8.2.E: Challenges of cybersecurity

Al-Aqla and Ali (2022) clarify a set of challenges for cybersecurity, including:

1. Mobile phone banking malware, which includes stealing financial information, bank details, and passwords.

2. Digital currencies: fake currencies, where cryptocurrency is bought and sold on cryptocurrency exchanges. The trader needs to open a trading account by filling out an online form. Most exchanges feature an order book that shows what traders are buying and selling and where they are performing this process.

3. Deepfake technology, through which victims are deceived by people accurately claiming other individuals through video or audio.

4. The threat of social engineering: using psychology to manipulate victims.

5. Internet of Things (IoT) devices, where a group of devices are linked together to perform a task or set of tasks. If these devices, or one of them, are hacked poses a threat to these tasks.

9. Study methodology:

The descriptive analytical approach was used for its suitability to the nature and objectives of the study. The study variables included digital education as an independent variable and the acquisition of cyber security skills as a dependent variable. Then the answers of students in the Faculty of Medicine at Al-Balqa Applied University on the study's questionnaire were analyzed to test the hypothesis and answer the questions.

9.1 Study population and sample:

The study population included all students of the Faculty of Medicine at Al-Balqa Applied University, whose number is (1886). The questionnaire was distributed electronically to the study population. After completing the distribution process, (150) answers were approved.

9.2 Study tool:

The study used the questionnaire as a tool for collecting primary data and was guided by the study variables and their measures, in addition to citing similar literature and studies related to the variables.

9.3 Validity of the study tool:

To ensure the validity of the study tool, it was presented to a number of faculty members at Jordanian universities to validate and express their opinions on it and the extent of the suitability and clarity of its items to the dimension to which it belongs, in addition to its ability to analyze statistically. Based on their opinions, suggestions, and modifications, some items have been modified. As a result, the study tool consisted of (30) items

Regarding construction validity, the questionnaire is characterized by constructive validity if its items measure what they were set to measure. This is done by analysing the Pearson correlation coefficient for this purpose based on (Sekaran, 2016) as shown in the following two tables:

Table 1: Correlation coefficient of the tool items within the digital education axis

The dimension	Item	Correlation coefficient on the axis	Correlation coefficient over the distance	The dimension	Number of items	Correlation coefficient over the distance	Correlation coefficient on the axis
Digital citizenship	1	.737**	.853**	Digital culture	11	.785**	.808**
	2	.681**	.794**		12	.727**	.796**
	3	.733**	.855**		13	.655**	.790**
	4	.727**	.818**		14	.676**	.804**
	5	.583**	.644**		15	.683**	.795**
Digital skills	6	.663**	.796**				
	7	.689**	.753**				
	8	.691**	.758**				
	9	.667**	.763**				
	10	.721**	.721**				

** The correlation is statistically significant at a level of 0.001

It is clear from the above table that the correlation coefficients of the items with their main dimensions and the total axis of the tool (digital education) is positive and statistically significant at a significant level of 0.001. Therefore, the indicators of the validity of the tool construction are high and suitable for the study according to the (Pearson) correlation coefficient as follows:

Table (2): Correlation coefficients of the items of the tool within the axis of acquiring cybersecurity skills

The dimensions	Item	Correlation coefficient on the axis	Correlation coefficient over the distance	The dimension	Item	Correlation coefficient over the distance	Correlation coefficient on the axis
Concepts of cyber security	16	.575**	.683**	**Cyber security challenges**	26	.684**	.766**
	17	.596**	.722**		27	.729**	.809**
	18	.710**	.832**		28	.789**	.846**
	19	.707**	.817**		29	.710**	.813**
	20	.689**	.779**		30	.775**	.819**
Cyber crimes	21	.727**	.807**				
	22	.732**	.859**				
	23	.719**	.892**				
	24	.680**	.823**				
	25	.779**	.887**				

The correlation is statistically significant at a level of 0.001

It is clear from the table above that the correlation coefficients of the items with their main dimensions and the total axis of the tool (the acquisition of cybersecurity skills) are positive and statistically significant at a significant level of 0.001. Therefore the indicators of the validity of the tool construction are high and suitable for the purposes of the study.

9.4 Reliability of the study tool

The reliability of the tool used to measure the variables (questionnaire) was confirmed by calculating the coefficient value (Cronbach's Alpha) using the SPSS software. The result was statistically acceptable if the coefficient's value was greater than or equal to (0.60) (Sekaran, 2016). Further, the closer the value to (1), i.e. 100%, the higher the reliability of the study tool. Given the results presented in Table (3), we found that the general reliability coefficient (Cronbach alpha) for the dimensions of the questionnaire was high, reaching (.873) for the total items. In contrast, the reliability of the dimensions ranged separately between (0.811) as a minimum and (.949) as a maximum. This means that the study tool (questionnaire) has a high degree of reliability and can be relied upon in the field application of the study.

Table (3): Cronbach alpha test results for the questionnaire items.

Dimensions	The number of items	Coefficient of internal consistency (Cronbach Alpha)
Digital education	15	.923
Digital citizenship	5	.846
Digital skills	5	.811
Digital culture	5	.857
Gain cyber security skills	15	.949
Concept of Cyber security	5	.826
Cyber crimes	5	.907
Challenges of Cyber security	5	.869
Total	30	.873

9.5 Normal distribution test

The researcher conducted a normal distribution test for the collected data. To ensure that it follows the normal distribution curve, the Skewness and the Kurtosis coefficient were calculated, assuming that if the values of Skewness and flatness are less than (1.960), the data is normally distributed with confidence (95%). The test information shown in Table (4) indicates that the data distribution was normal, as the values of the torsion coefficient were less than (1.960) for all study variables.

Table (4): The normal distribution of the data depending on the skewness coefficient

Variables' type	Variables and dimensions	Kurtosis coefficient	Standard deviation	Kurtosis value	Flattening coefficient	Standard deviation	Kurtosis value
Indep variables	Digital education	.073-	.177	0.412-	.207-	.353	0.586-
	Digital citizenship	.337-	.177	1.903	.141-	.353	0.399-
	Digital skills	.127-	.177	0.717-	.351-	.353	0.994-
	Digital culture	.063-	.177	0.355-	.691-	.353	1.957-
Depend variables	Gain cyber security skills	.116	.177	0.655	.408-	.353	1.155-
	Concept of Cyber security	.046	.177	0.259	.524-	.353	1.484-
	Cyber crimes	.034-	.177	0.1920-	.614-	.353	1.739-
	Challenges of Cyber security	.236-	.177	1.333-	.144-	.353	0.407-

Table (5) refers to the (One-Sample Kolmogorov-Smirnov Test) to illustrate the normal distribution of the study data.

	Digital education	Digital citizenship	Digital skills	Digital culture	Gain cyber security skills	Concept of Cyber security	Cyber crimes	Challenges of Cyber security
Kolmogorov-Smirnov Z	.482	1.617	1.070	.960	.955	1.135	.949	.985
Asymp. Sig. (2-tailed)	.974	.011	.202	.316	.321	.152	.329	.287

Table (5) shows that the data follows a normal distribution by calculating the (Kolommogorv-Smirnonz) test. This was achieved as the values reached (482 to 1.617), where the value of (Sig) was bigger than (0.05), which is at the significance level ($\alpha \leq 0.05$) adopted in the state of the statistical process of this study (Gujarati, Porter and Sangeetha, 2017).

10. The results of the data analysis and hypothesis test

10.1 Description of the demographic characteristics of the study sample

This section describes the study sample's demographic characteristics, including gender and years of work experience. Table (6) shows the distribution of sample members by gender.

Table (6) Frequencies and percentages determined for the study sample by gender

Gender	Repetition	Percentages %
Male	91	60.66
Female	59	39.34
Total	150	100.0

It is clear from the results of Table (6) that the distribution of the study sample, according to the gender variable, the largest category of the sample is males, with a percentage of (60.66%), with (91) students.

10.2 Arithmetic means and standard deviations

This part reviews the responses of the study sample to the questionnaire items related to the dimensions of digital education (digital citizenship, digital skills, digital culture) as an independent variable and the dimensions of acquiring cybersecurity skills (the concept of cybersecurity, cybercrime, challenges of cybersecurity) as a dependent variable through measuring the arithmetic mean and standard deviation for each item separately.

10.3 First: Description of the dimensions of digital education

Table (7): Description of the dimensions of digital education

Dimensions	**Arithmetic means**	**Arrangement of the importance of the items**	**Evaluation level**
Digital citizenship	2.85	2	average
Digital skills	2.99	1	average
Digital culture	2.74	3	average
Digital education	3.7426		average

Table (7) shows that the level of digital education among students of the Faculty of Medicine at Al-Balqa Applied University was average. The arithmetic mean of the answers of the study sample in digital education was (3.7426). It also appears from the table that the arithmetic means of the estimates of the study sample on the dimensions of digital education were average for all dimensions. The "digital skills" dimension came first, with an arithmetic mean of (2.85), with a high evaluation score, whereas "Digital Culture" came in last, with an arithmetic mean of (2.74), with an average evaluation score.

10.4 First dimension digital citizenship

Table No. (8): Arithmetic means and standard deviations of the respondent's answers to the items of (Digital Citizenship)

No	**Item**	**Arithmetic means**	**Standard deviation**	**Order of importance**	**Evaluation level**
1	My family promotes my culture through the good use of digital technologies	2.94	0.725	1	average
2	I know my rights and duties while surfing the Internet	2.87	0.711	2	average
3	I use social media consciously and responsibly	2.83	0.700	3	average
4	I do not overuse digital devices because it leads to digital addiction.	2.81	0.697	4	average
5	I know digital laws and legislation in the country	2.80	0.780	5	average
Total digital citizenship		2.85	average		

Table (8) indicates that the general indicator has reached (2.85) on the total digital citizenship scale, which reflects the average level of importance, according to the respondents. It is noted from Table (8) that item (1), which states: My culture in the good use of digital technologies," came in the first place with an arithmetic mean of (2.94), which reflects an average level of importance. On the other hand, item (5), "I know digital laws and legislation in the country," had the lowest arithmetic mean, which amounted to (2.80), reflecting an average level of importance.

10.5 Second: digital skills

Digital skills is one of the dimensions of digital education, where the arithmetic means and standard deviations were calculated for the study sample's responses to the digital education items of the students of the Faculty of Medicine at Al-Balqa Applied University.

Table No. (9): Arithmetic means and standard deviations of the respondent's answers to the items (digital skills)

NO	Items	Arithmetic means	Standard deviation	Order of import ance	Evaluati on level
6	I am good at studying through digital study engines to reach the authenticity of the information.	3.49	0.725	2	Average
7	I use search engines which support the language to access the information.	3.55	0.711	1	Average
8	My use of digital media enhances my communication with others.	2.86	0.700	3	Average
9	I communicate with others through social media.	2.74	0.697	4	Average
10	I choose the appropriate level in adjusting the screen brightness and brightness levels for the digital devices I use.	2.56	0.780	5	Average
Total digital skills		2.99	Average		

Table (9) shows that the general indicator has reached (2.99) on the digital skills scale, which reflects an average level of importance, according to the respondents. It is noted from Table (9) that item (7), which states, "Ise search engines that support the language to access the information," came first with an arithmetic means of (3.55), which reflects an average level of importance. On the other hand, item (10), which states: "Choose the appropriate level in adjusting the screen brightness and brightness levels for the digital devices I use." had the lowest arithmetic mean, which amounted to (2.56), reflecting an average level of importance.

10.6 Third: digital culture

Table No. (10): Arithmetic means and standard deviations of the respondent's answers to the items (Digital Culture)

NO	Item	Arithmetic means	Standard deviation	Order of importance	Evaluation level
11	I make sure that the information is correct by referring to its sources.	2.55	0.805	4	Average
12	I learn by surfing the internet	2.86	0.831	3	Average
13	I prefer to deal with well-known websites.	2.54	0.793	5	Average
14	I adhere to elegant and civil behavior rules when dealing with digital applications.	2.70	0.916	2	Average
15	Attending seminars and educational programs enhances my ways of benefiting from digital technologies.	3.10	0.757	1	Average
Total digital culture		2.74	Average		

Table (10) indicates that the general indicator has reached (2.74) on the total scale of digital culture, and it reflects an average level of importance, according to the respondents. It is noted from the table that item (15), which states: "Attending seminars and educational programs enhances my ways of benefiting from digital technologies," came first with an arithmetic mean of (3.10), which reflects an average level of importance. In contrast, item (13) "I prefer to deal with well-known websites" reached (2.54), which reflects an average level of importance.

10.7 Second: Description of the dimensions of acquiring cybersecurity skills (the dependent variable)

The dependent variable in the study is the acquisition of cybersecurity skills. To determine the relative importance of acquiring cybersecurity skills and its dimensions (the concept of cybersecurity, cybercrime, challenges of cybersecurity) and to answer the second study question (What is the relative importance of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University?) Arithmetic means and standard deviations were calculated to identify the responses of the study sample on the level of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University.

Table (11) The arithmetic means and standard deviations of the study sample's responses to the dimensions of acquiring cybersecurity skills

Dimensions	Arithmetic means	Arrange the importance of the items	Evaluation level
Concept of Cybersecurity	3.6053	1	Average
Cyber crimes	3.3479	3	Average
Challenges of Cybersecurity	3.4383	2	Average
Gain cyber security skills	3.4638	Average	

It appears from Table (11) that the level of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University was average. The arithmetic mean of the answers of the study sample on the field of acquiring cybersecurity skills as a whole was (3.4638). It is also clear from the table that the arithmetic means of the estimates of the study sample on the dimensions of acquiring cybersecurity skills ranged between (3.6053 - 3.3457) with an average evaluation score for all Dimensions. The "Concept of Cyber Security" dimension first, with an arithmetic mean (3.6053) and an average evaluation score, while in the last place came " with an arithmetic mean (3.3401), with an average evaluation score.

In order to identify the importance of each dimension of acquiring cybersecurity skills for students of the Faculty of Medicine at Al-Balqa Applied University, according to its items, the arithmetic means and standard deviations were calculated, and the following are the results.

10.8 The concept of cybersecurity

The concept of cybersecurity is one of the dimensions of acquiring cybersecurity skills, where the arithmetic averages and standard deviations were calculated for the responses of the study sample on the items on the concept of cybersecurity among the students of the Faculty of Medicine at Al-Balqa Applied University.

Table (12): The arithmetic means and standard deviations of the respondents' answers to the items (the concept of cybersecurity)

NO	Item	Arithmetic means	Standard deviation	Order of importance	Evaluation level
16	I make sure of rumors in the digital community in order to preserve community security.	3.4255	.96450	1	Average
17	I Make sure that the browser I use is safe	3.2766	1.06880	5	Average
18	I provide my personal computer with antivirus software.	3.2766	1.03835	4	Average
19	Protect my data by creating my own password	3.3404	1.01910	3	Average
20	Respect the property rights of others.	3.4202	1.04396	2	Average
Total concept of cyber security		3.6053	.73925	Average	

Table (12) shows that the general indicator has reached (3.6053) on the scale of the concept of cybersecurity, which reflects an average level of importance, according to the respondent's view. It is noted from the Table that item (16), which states "I make sure of rumors in the digital community in order to preserve community security," came first with an arithmetic mean of (3.7819), which reflects an average level of importance. On the other hand, item (17), which states: "I Make sure that the browser I use is safe," got the lowest arithmetic mean of (3.4415), which reflects an average level of importance.

10.9 Cybercrimes

Cybercrime is one of the dimensions of acquiring cybersecurity skills. Arithmetic averages and standard deviations were worked out for the study sample's responses to the cybercrime items of the students of the Faculty of Medicine at Al-Balqa Applied University.

Table No. (13): Arithmetic means and standard deviations of the respondent's answers to the paragraphs (cybercrime).

No	Item	Arithmetic means	Standard deviation	Order of importance	Evaluation level
21	I am careful when using Visa cards and prepaid cards.	3.4255	.96450	1	Average
22	I respect the other person's point of view via digital media and their disagreement with mine	3.3404	1.01910	3	Average
23	I know well the legal risks of violating the privacy of others	3.2766	1.03835	4	Average
24	I realize the dangers of using piracy and hacking software.	3.4202	1.04396	2	Average
25	Sending annoying e-mails to others is considered immoral.	3.2766	1.06880	5	Average
Total cybercrime		3.3479	.87731	Average	

Table (13) indicates that the general indicator has reached (3.3479) on the total scale of cybercrime, which reflects an average level of importance, according to the respondents. It is noted from Table (13) that item (21) (I am careful when using Visa cards and prepaid cards) came first with an arithmetic mean of (3.4255), which reflects an average level of importance. On the other hand, item (25) (Sending annoying e-mails to others is considered immoral) got the lowest arithmetic mean of (3.2766), which reflects an average level of importance.

10.10 Challenges of the Cybersecurity

Cybersecurity challenges are one of the dimensions of acquiring cybersecurity skills, where the arithmetic means and standard deviations were calculated for the responses of the study sample on the items of acquiring cybersecurity skills among the students of the Faculty of Medicine at Al-Balqa Applied University.

Table No. (14): Arithmetic means and standard deviations of respondent's answers to the items (challenges of the Cybersecurity)

No	Paragraph	Arithmetic means	Standard deviation	Order of importance	Evaluation level
26	I ensure the security of commercial websites by studying the HTTP code and the lock icon.	3.5213	1.03137	2	Average
27	I don't deal with cryptocurrencies, as it doesn't represent security for me and aren't clear	3.5691	.96489	1	Average
28	I can discern deep fake technology and how to use it	3.4043	1.05789	3	Average

29	I follow the latest cyber security breaches to learn about them and protect myself	3.3936	1.04158	4	Average
30	I avoid using my personal social media accounts on public devices	3.3032	1.07404	5	Average
Total challenges of the Cybersecurity		3.4383	.83827	Average	

Table (14) indicates that the general indicator has reached (3.343147) on the scale of challenges of Cybersecurity, which reflects an average level of importance, according to the respondents. It is noted from the table that item (27) "I don't deal with cryptocurrencies, as it doesn't represent security for me and aren't clear) won the competition using an arithmetic mean of (3.5213), which implies an average level of importance. On the other hand, item (30), which states, "I avoid using my personal social media accounts on public devices" got the lowest arithmetic mean (3.3032), which reflects an average level of importance.

11. Testing the study hypothesis:

The hypothesis: Ho1: There is no statistically significant effect at level ($\alpha \leq 0.05$) of digital education with (digital citizenship, digital skills, digital culture) on acquiring cybersecurity skills with its combined dimensions (concept of the cybersecurity, cybercrime, challenges of the cybersecurity) among students of the Faculty of Medicine at Al-Balqa Applied University. Before testing the hypothesis and regression analysis, it is required to test the validity of the data for statistical analysis and the absence of a multicollinearity problem between the independent variables. Thus it was subjected to the multicollinearity test, which calculates two important indicators:

1. Variance Inflation Factor (VIF): There is inflation if the value of (VIF) is equal to 10 or more.

2. Tolerance: the value must be 0.1 or more.

Table No. (15): Coefficient of Variance Inflation Test and Tolerance Coefficient

Model	Collinearity Statistics	
	Tolerance	VIF
digital citizenship	.464	2.153
digital skills	.380	2.634
digital culture	.461	2.170
Dependent Variable: Decision Making		

Table No. (16): summary of the linear model of the relationship between digital education and the acquisition of cybersecurity skills

Model Summary[b]						
Durbin-Watson	Std. The error of the Estimate	Adjusted R Square	R Square	R	Model	
1.884	.49032	.546	.553	.744[a]	1	
ANOVA[a]						
Sig.	F	Mean Square	df	Sum of Squares	Model	
.000[b]	76.027	18.278	3	54.835	Regression	1
		.240	184	44.237	Residual	
			187	99.071	Total	
Coefficients[a]						
Sig.	T	Standardized Coefficien	Unstandardized Coefficient		Model	
		Beta	Std. Error	B		
.003	2.999	.217	.075	.226	gital citizenship	1

.153	1.435	.115	.083	.119	digital skills	
.000	6.788	.493	.070	.475	digital culture	
a. Dependent Variable: Gaining cyber security skills						

Table (16) shows that there is a direct relationship to test the main hypothesis. There is no statistically significant effect at the level ($\alpha \leq 0.05$) of digital education with its dimensions (digital citizenship, digital skills, digital culture) in acquiring cybersecurity skills in terms of its dimensions combined. The concept of cybersecurity, cybercrime and the challenges of cybersecurity among students of the Faculty of Medicine at Al-Balqa Applied University. The value of the correlation coefficient was (.744a) (R), which is a statistically significant value that indicates a statistically significant correlation between the independent variables and the dependent variable. The value of R-square (55.3) is statistically significant, which explains the ability of digital education dimensions to influence the acquisition of cybersecurity skills. It showed a coefficient of statistical significance (0.000), meaning that the dimensions of digital education accounts for (55.3%) of the change in the acquisition of cybersecurity skills. The value of the test was (76.027) (F), with a statistical significance of (0.00). It is a statistically significant value indicating that there is a variation in the ability of the independent variables to influence the dependent variable. Also, through the coefficients table, it is shown that the values of (B) in the digital citizenship dimension were (226), and the value of (t) was (2.999) with a significance level of (.003). This indicates that the dimension is significant. The value of (B) in the dimension of digital skills has reached (119), and the value of (t) was (1.435) with a significance of (.153). This implies that the dimension is not significant. The value of (B) in the digital culture dimension reached (.475), and the value of (t) (6.788) at a significance level of (.000). This indicates that the dimension is significant. Therefore, the main hypothesis is rejected by the zero formula and the alternative formula is accepted, which states that there is a statistically significant effect at a significant level ($\alpha \leq 0.05$) of digital education with its dimensions (digital citizenship, digital skills, digital culture) in acquiring cybersecurity skills with its dimensions combined (The concept of cybersecurity, cybercrime, cybersecurity challenges) among students of the Faculty of Medicine at Al-Balqa Applied University.

12. Results

The results showed that the level of digital education among the students of the Faculty of Medicine at Al-Balqa Applied University was average. It also appears from the tables that the arithmetic means of the estimates of the study sample on the dimensions of digital education came, respectively, in the first place “digital skills” with average evaluation score. The digital citizenship dimension came second with an average evaluation, while “digital culture” came last, with an average evaluation score. This may be due to educational initiatives targeting this young group to increase their awareness, culture, digital citizenship, and digital skills. Also, results also showed that the level of acquiring cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University was average. The concept of cybersecurity came in first place with an average rating; secondly came the challenges of cybersecurity with an average rating, whereas “Cyberspace Crimes” came in last place with an average rating. This can be explained by the prevalence of individual or collective behaviors and the spread of electronic crimes, such as exposure to electronic fraud, blackmailing, piracy, bullying, and data theft, which increased society’s awareness of cybersecurity challenges and crimes. To add more, results also showed a statistically significant effect at a significant level ($\alpha \leq 0.05$) of digital education with its dimensions (digital citizenship, digital skills, digital culture) in acquiring cybersecurity skills with its combined dimensions (the concept of cybersecurity, cybercrime, security challenges cyber) among students of the Faculty of Medicine at Al-Balqa Applied University.

13. Recommendations

Based on the findings, this study recommends the following: Preparing and conducting the necessary courses, seminars, and workshops on a continuous and regular basis for students, especially with regard to the dimensions of digital education (digital citizenship, digital culture and digital skills). Furthermore, enhancing the acquisition of cybersecurity skills among students of the Faculty of Medicine at Al-Balqa Applied University through raising and increasing students' understanding of cybersecurity and increasing the courses offered to them in the field of digital laws and various digital skills. Moreover, conducting future studies on digital education and its implications on acquiring cybersecurity skills among a sample of public school students. Additionally, the study also suggests conducting future studies that clarify the impact of digital education in crisis management.

References

Abuanzeh, A.A., Qtaishat, G.M., Sakher, S., Al-eassa, A.A., Alshurideh, M. (2023). The Role of Strategic Entrepreneurship Requirements in Promoting Competitive Advantage at Al-Balqa Applied University. In: Hassanien, A.E., Snášel, V., Tang, M., Sung, TW., Chang, KC. (eds) Proceedings of the 8th International Conference on Advanced Intelligent Systems and Informatics 2022. AISI 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 152. Springer, Cham. https://doi.org/10.1007/978-3-031-20601-6_44

Ahmed et al. (2022). Cyber security and digital hygiene. Egyptian Journal of Information Sciences, 9(2), 390-422.

Al-Aqla et al. (2022). The degree of awareness of cybersecurity concepts among male and female computer teachers in Hail. Arabic Studies in Education and Psychology, (144), 279-300.

Al-Haddad, Nabila (2022). Requirements for achieving cybersecurity in Yemeni university libraries: a case study. Al-Bayda University Journal, 4 (2), 25-39.

Al-Manthari, Fatima (2020). The role of school leadership in enhancing cybersecurity in government schools for girls in Jeddah from the point of view of female teachers. Arab Journal of Educational and Psychological Sciences, 4 (17), 457-484

Al-Sawat, Hamad and Al-Manea, Noura (2020). The relationship between awareness of cybersecurity and national, moral and religious values among students of the elementary and intermediate stages in Taif City, Journal of the Scientific Study in Education, (21), 278-306.

Awad et al. (2020). The role of digital education in empowering the early childhood teachers with twenty-first-century skills. Journal of Childhood and Education, 4 (41), 115-187.

Cham, K., Edwards, M.-L., Kruesi, L., Celeste, T. & Hennessey, T. (2021). Digital preferences and perceptions of students in health professional courses at a leading Australian university: A baseline for improving digital skills and competencies in health graduates. Australasian Journal of Educational Technology, 69–86. https://doi.org/10.14742/ajet.6622

Ghavifekr, Simin (2022), Technology Leadership in Malaysian Schools: The Way Forward to Education 4.0 – ICT Utilization and Digital Transformation, International Journal of Asian Business and Information Management (IJABIM), 13(2),1-18.

Khalifa, Ali (2022). The impact of the different styles of presentation of educational infographics (static/mobile/interactive) on the development of digital citizenship concepts among high school students and their attitudes towards it. Fayoum University Journal of Educational and Psychological Sciences, (12), 15-32.

Naziha et al. (2021). The reality of smart digital education in rehabilitation programs for people with special needs. The Pedagogical Center for Handicapped Children in Biskra as a model. Scientific Journal of Technology and Disability Sciences, 1 (3), 149-169.

Saileela, K. and Kowsalya,M. (2021), Knowledge on Digital Skills and Usage of Social Sites among B.Ed. Students, The International journal of analytical and experimental modal analysis, 3 (3),1338- 1349

Sakher, S., Al Fouri, A., Al Fouri, S., Alshurideh, M.T. (2023). The Reality of Artificial Intelligence Skills Among Eighth-Grade Students in Public Schools. In: , et al. The 3rd International Conference on Artificial Intelligence and Computer Vision (AICV2023), March 5–7, 2023. AICV 2023. Lecture Notes on Data Engineering and Communications Technologies, vol 164. Springer, Cham. https://doi.org/10.1007/978-3-031-27762-7_9

Waliyuddin, D. S., & Sulisworo, D. (2022). High Order Thinking Skills and Digital Literacy Skills Instrument Test. Ideguru: Jurnal Karya Ilmiah Guru, 7(1), 47-52. https://doi.org/10.51169/ideguru.v7i1.310