Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Awareness of electronic crimes related to E-learning among students at the University of Jordan

Hani Y. Ayyoub [a,*], Ahmad A. AlAhmad [b], Amani Al-Serhan [c], Mohammad F. Al-Abdallat [d], Esra'a Al-Muheisen [e], Hadeel Boshmaf [c], Yasmeen A. Abu-Taleb [f], Yarob O. Alqudah [g], Yazan Alshamaileh [a]

[a] *King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan*
[b] *Information Technology Center, The University of Jordan, Amman, Jordan*
[c] *Center for Women's Studies, The University of Jordan, Amman, Jordan*
[d] *School of Educational Sciences, The University of Jordan, Amman, Jordan*
[e] *Language Center, The University of Jordan, Amman, Jordan*
[f] *School of Languages, The University of Jordan, Aqaba, Jordan*
[g] *University Requirements Coordination Office, The University of Jordan, Amman, Jordan*

ARTICLE INFO

Keywords:
Technology
Education
E-learning
Cybercrime
Legal

ABSTRACT

The spread of e-learning as an alternative to traditional or face-to-face education has faced many problems and challenges in general and ethical and legal challenges in particular. This study aims to measure students' awareness of the safe use of technology and its tools in e-learning that is consistent with ethical and legal standards. The study attempts to reveal the degree of awareness of students of the University of Jordan about electronic crimes related to e-learning and the legal procedures and penalties related to electronic crimes in e-learning. Quantitative research methods were used. A questionnaire was established and distributed to students enrolled in the following online courses: Ethics and Human Values, Communication Skills, and National Culture. Analysis of the data revealed that students had a high awareness about cybercrime due to the widespread use of the internet by students as it became an integral part of their daily lives. The degree of awareness of student about legal procedures and penalties related to electronic crimes in e-learning was medium. This indicates students' lack of awareness of the effectiveness of procedures and penalties for electronic crimes that can be applied in e-learning due to the rapid transition in the learning process at the University of Jordan from traditional learning to distance e-learning that was imposed during the Corona pandemic. Based on these findings, the study presented a set of recommendations that could be implemented to increase awareness and maximize the benefit of using e-learning.

1. Introduction

Many aspects of our lives are employing digital networks and increasingly indulging in the online environment especially during the recent Corona pandemic that the whole world continues to fight. Although education is one of the most affected fields by the pandemic, e-learning and its virtual world offers a socially interactive alternative for learners at all levels. Nonetheless, e-learning has become a fertile environment where dangerous acts are practiced. A diverse range of crimes are committed on e-learning platforms. These crimes have adopted new forms, new scenes, and new tools. Cybercrimes in e-learning are thus receiving a growing space in criminology.

Cybercrimes are defined as illegal activities that can only be performed using a computer, computer networks, or other forms of information communication technology (Maimon and Louderback, 2019). A report by James Lewis in 2018 concludes that cybercrimes are noticeably increasing as the global losses to cybercrimes are about $600 billion compared to $445 billion in 2014. Furthermore, the report suggests that the growth of cybercrimes over the years is enhanced by the growth of the black market and digital currencies (Lewis, 2018). discusses different

[*] Corresponding author.
E-mail address: H.ayyoub@ju.edu.jo (H.Y. Ayyoub).

https://doi.org/10.1016/j.heliyon.2022.e10897
Received 23 February 2022; Received in revised form 24 May 2022; Accepted 28 September 2022

types of cybercrimes including intellectual property theft, identity theft, business email compromise, and other financial cybercrimes. These crimes need new policies and laws to lower their risks. Nonetheless, this paper mainly focuses on cybercrimes that are related to e-learning.

In e-learning, information is more vulnerable to threats since in cyberspace events occur almost instantaneously across large distances, network boundaries do not align with physical and political boundaries and digital environments are subject to attacks from a wide range of locations (Balkin et al., 2007). Therefore, some users have exploited e-learning platforms to gain unauthorized access to information systems that are used by educational institutions, teachers, and students.

2. Objectives of the study

This study aims to measure students' awareness of the safe use of technology and its e-learning tools that are consistent with ethical and legal standards. The study attempts to reveal the degree of awareness among students at the University of Jordan about electronic crimes related to e-learning and the legal procedures and penalties related to electronic crimes in e-learning.

2.1. Research questions

1. What is the degree of awareness of students at The University of Jordan regarding electronic crimes related to e-learning?
2. What is the degree of awareness of students at The University of Jordan about the legal procedures and penalties related to electronic crimes in e-learning?
3. What are the statistical variations (at the level of significance ($\alpha = 0.05$)) regarding the degree of awareness of electronic crimes in e-learning among students of the University of Jordan based on study variables (course, gender, and faculty)?
4. What are the statistical variations (at the level of significance ($\alpha = 0.005$)) regarding the degree of awareness of legal procedures and penalties related to electronic crimes in e-learning among students of the University of Jordan based on the study variables (course, gender, and faculty)?

3. Background and literature review

Ever since its establishment in the 1960s, e-learning has evolved in numerous ways. While there is no single definition for e-learning as it varies depending on context (Campbell, 2004), e-learning in higher education has come to be defined as the use of both software-based and online learning (Kidd, 2009). According to (Urdan and Weggen, 2000), e-learning covers a wide set of applications and processes, including computer-based learning, web-based learning, virtual classrooms, and digital collaborations (Kidd, 2009; King et al., 2009). Other scholars narrowed the definition of e-learning to forms of learning that are dependent on the internet or web based (Keller and Cernerud, 2002; LaRose et al., 1998). As a concept, e-learning includes a wide array of applications, learning methods and processes (Rossi, 2009). (Wentling et al., 2000) concur that e-learning can be seen as the acquisition and use of knowledge distributed and facilitated primarily by electronic means. E-learning as a medium of education is timeless and spaceless, with the potential of reaching students across the globe. It provides learners with vast knowledge and opportunities to connect socially in ways that traditional settings could not. The possibility of knowledge sharing and interconnectedness in numerous formats creates a rich environment and medium for learning (Kidd, 2009).

3.1. Types of e-learning

There are various ways to classify e-learning depending on the level of engagement in education and to the timing of the interaction (Algahtani, 2011). Some scholars divided e-learning into two basic types, consisting of computer-based and the internet based e-learning (Algahtani, 2011). Computer-based learning involves using a variety of hardware and software that are available in Information and Communication Technology (ICT). Furthermore, this learning mode could be subdivided into computer-managed instruction and computer-assisted learning. In the first type, computers are utilized to store and retrieve information to support the management of education, whereas the latter type involves the use of computers as an alternative to traditional methods, relying mainly on interactive software as a support tool within the class or as a tool for self-learning outside the class (Arkorful and Abaidoo, 2015). Internet-based learning, however, is a more advanced mode in making course contents available on the internet, with the readiness of links to related knowledge sources, for examples e-mail services and references which could be used by learners at any time and place as well as the availability of teachers or instructors (A. Almosa, 2002).

Other classifications of the types of e-learning vary depending on the extent of using the internet or computer assisted learning. Thus, e-learning could consist of blended (or mixed) learning, assistant mode, or completely electronic (Zeitoun, 2008). The assistant mode supports traditional methods when necessary and blended mode offers a short-term degree for a partly traditional method. However, the completely online mode involves the exclusive use of the network for learning (Zeitoun, 2008). The latter type is further classified as synchronous or asynchronous based on the timing of interaction (Algahtani, 2011). The synchronous involves alternate online access between teachers or instructors and learners, or between learners, and the asynchronous, allows all participants to post communications to any other participant over the internet (Algahtani, 2011; A Almosa and Almubarak, 2005). During synchronous settings, students can have discussions and interactions with their instructors and among themselves through the internet at the exact moment via various tools such as the video conference and chat rooms allowing them to benefit from instantaneous feedback (A Almosa and Almubarak, 2005). Whereas asynchronous mode while allowing students to interact with instructors, is not instantaneous and is usually done using tools such as thread discussion and emails (Algahtani, 2011; A Almosa and Almubarak, 2005). Thus, it enables students to learn at a time of their convenience, with the lost advantage of benefiting from instant feedback from either instructors or fellow colleagues (A Almosa and Almubarak, 2005).

3.2. E-learning amid COVID-19

The COVID-19 pandemic has affected the education system with a severe impact on students, lecturers, and educational organizations around the globe (Mailizar et al., 2020). The pandemic caused a disruption and a shift in the educational forms transferring it from conventional classroom instruction with traditional methods to delivering courses to students at a distance using technology or, namely, online learning (Gonzalez et al., 2020; Toquero, 2020). The COVID-19 pandemic has also focused on the vital role of technology in creating productive opportunities for transformation in teaching and learning styles, tools, and approaches (Raheem and Khan, 2020). However, this rapid transformation requires considerable attention to the various obstacles and challenges of integrating educational technology and e-learning strategies in education (Crawford et al., 2020).

Several studies have addressed the deficiencies of electronic learning initiatives mainly because of the absence of preparation for this experience by institutions and their constituents (Aydın et al., 2005; Borotis and Poulymenakou, 2004). The lack of resources in academic institutions, insufficient access, availability, affordability, and reliable internet connections have been the main issues that affect organizational responsiveness (Salahshouri et al., 2022; Zhong, 2020). Some studies even questioned the capacity to successfully teach digitally (Liguori and Winkler, 2020).

Other researchers investigated the students themselves, their internal struggles, and the perceived barriers to online learning (Marino et al., 2000). noted that students may suffer from difficulty adjusting, managing, and maintaining self-motivation within the structure of online courses. Students are missing social activities and interactions that are necessary for growth and learning in educational institutions (Adnan and Anwar, 2020). Moreover, evidence of depression, anxiety, and stress symptomatology has been recorded among undergraduate student due to this surge of instruction methods and growth of stressful workloads on the students (Fawaz and Samaha, 2021). The pressures of the sudden changes to existing pedagogies and practices cause difficulties for students in adjusting to innovations and enhancements of existing ones (Watkins et al., 2004).

Research also addresses a number of security concerns, requirements, and best practices to consider when using online educational services. Investigating security risks and protection along with cybercrime, has been growing in recent years especially during the COVID-19 pandemic where many systems associated with educational institutions have also become victims of cybercrimes given the absence of careful planning or understanding of the security aspects of online learning (Alwi and Fan, 2010). In online learning, security means that learning resources are available and unimpaired to all authorized users when they are needed and are subsequently protected from malicious or accidental misuse (Adams and Blanford, 2003). Another major challenge to e-learning is the credibility and equality of the online assessments to largely ascertain students' progress (Reeves, 2000). Cheating, according to students, is easier in an online environment than in a conventional one (King et al., 2009). Students can have a wider range of tools and methods of cheating in online assessments ranging from taking the same assessment several times and receiving unauthorized help (Rowe, 2004), online communications, telecommunication, internet surfing (Rogers, 2006), copying and pasting from online sources (Underwood and Szabo, 2003). Hence, the security of online assessments is an essential element in the security of online learning. It is thus harder to prevent cheating in online course assessments than in traditional classrooms (Ndume et al., 2008).

In order to alleviate security threats and risks during online learning, a variety of proposals have been suggested encompassing several perspectives (Srivastava and Sinha, 2013). advocate strongly for improving security knowledge and skills in information security through professionals by implementing the Virtual Training Environment (VTE), a web-based knowledge library launched by the Carnegie Mellon Software Engineering Institute (Alwi and Fan, 2010). recommend information security management (ISM) for online learning providers, comprised of an effective security architecture that can effectively challenge existing and emerging information security threats. They argue that ISM should include policies, processes, procedures, organizational structures, and software and hardware functions, to enhance the execution of security measures.

3.3. E-learning amid COVID-19 in Jordan: opportunities and challenges

During the COVID-19 crisis, Jordanian universities were required to offer online materials and give online lectures. Universities use various platforms to live broadcast lectures such as Skype, Google Classroom, Moodle, Zoom, and Facebook. Universities are also required to provide the Ministry of Higher Education and Research with the number of courses that were converted to online and the number of students who log on to universitys' online learning platforms (Shahroury, 2022).

Some of the challenges which appeared through e-learning during COVID-19 are related to poor infrastructure, students' inability to access necessary software, and fear of public appearance on e-learning platforms due to some traditions and norms. A published study emphasized that although e-learning is an effective and well managed learning method, it cannot completely replace traditional face-to-face teaching, especially in the clinical year of medical schools (Al-Bdour, AlShawabkeh, Alni'mat, AlRyalat and Abuameerh, 2022; Barakat et al., 2022).

When writing about the opportunities during COVID-19, we find that Jordan has benefited from UNHCR which runs a network of 10 connected learning hubs throughout Jordan, supported by Google. org" title = "http://Google.org">Google.org and Learning Equality and operated by local NGO, JOHUD (the Jordanian Hashemite Fund for Human Development). The learning hubs offer advanced education courses for both refugee youth and Jordanian nationals aged 13–17 years old (Carlisle, 2020). Furthermore, students and faculty members at universities became more skilled after COVID-19 with using e-learning platforms, and became highly qualified after joining many courses on how to use the e-learning platforms and solve the technical issues they might encounter (Alsoud and Harasis, 2021).

3.4. Major challenges with E-learning

Despite the wide use of e-learning across the globe and particularly during the COVID-19 pandemic, many concerns were raised regarding its efficiency in providing students with sound knowledge and skills. While e-learning has been lauded as a successful teaching medium and methodology, particularly in the case of the global pandemic, many challenges emerged about its long-term use. These include learners experiencing feelings of alienation and a lack of interaction. These are further aggravated if the learners do not possess the necessary skills to contribute in the process of knowledge sharing and academic interaction among peers and instructors. Consecutively, it may negatively impact socialization skills and limit the role of instructors as directors of the educational process (Arkorful and Abaidoo, 2015). E-learning as a teaching method may prove to be less productive than face-to-face interactions for clarifications, explanations, and interpretations. As students become more adept to e-learning, many unwarranted phenomena become more visible. These include cheating, piracy, and plagiarism.

While e-learning has proved to be successful across many disciplines, other disciplines cannot effectively benefit from e-learning including scientific fields that require practical experience that is difficult to translate online. This is why researchers have argued that e-learning is more appropriate in social sciences and humanities than other fields such as medical science and engineering where there is the need to develop practical skills (Arkorful and Abaidoo, 2015).

3.5. Cybercrimes

3.5.1. The evolvement of the term cybercrime

With the rapid development of technology, it has become crucial to protect ourselves from cybercrimes as this evolution can be abused by attackers taking advantage of users' lack of awareness. Thus, it imposes one of the most significant risks in economic, political, educational, social, and other sectors in life. From a holistic approach, a cybercrime is any criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity, and include everything from electronic cracking to denial-of-service attacks. It also includes traditional physical crimes where computers or networks are used to enable illicit activity (Gandhi and Thanjavur, 2012). However, it can be challenging to decide on one unified definition of what cybercrimes are as some definitions are relatively narrow on focus (Petee et al., 2010); meaning they are limited to one type; therefore, it cannot be used widely.

The massive and rapid technological development has contributed, with its technical means, to the emergence of a new type of crime known as cybercrime. At the beginning of the spread of this type of crime and before the advent of internet networks and modern means of communication, some jurisprudence used the term computer fraud (Kunz and Wilson, 2004) to refer to these crimes as it was most common when these behaviors emerged. However, the term quickly became unsuitable for the nature of the crime since fraud is considered a type of crime, not a term that could be used as a whole. Afterward, the term computer crime (Kunz and Wilson, 2004) came to refer to criminal activities using a computer, a similar device, a spreadsheet, or data contained therein. However, this term is not precise because it only focuses on an essential element used in the crime (i.e., the computer), thus neglecting other tools used in such crimes. Furthermore, the general term covers crimes committed against physical components of a computer on the one hand, and the other excludes crimes committed where the computer is merely a tool to carry out a criminal act such as fraud.

Another term, computer misuse (Kerr, 2003), appeared to include more significant computer-related issues, but the term was inaccurate because some computer-based malpractice might not amount to a criminal offense, and many crimes were committed through legitimate computer use. Then, the term ICT crime emerged as an attempt to cover all related crimes, but it was also not inclusive as it excluded crimes where the device was not connected to a particular network.

Many terms and expressions have emerged to identify and define these crimes; however, the rapid technological development and the information revolution which has created computers, supporting devices, and tools, followed by information systems, the internet, applications, and software, made it challenging to keep up with these criminal developments and practices. Eventually, the term cybercrimes emerged, but a specific definition is subject to controversy. Hence, no consensus on the definition of such crimes has been reached. The Jordanian legislature has used the term cybercrime (Jordan, 2015) in Cybercrimes Law without defining such crimes; nevertheless, Article (2) of the law sets out concepts that may help us define such crimes that are consistent with the Jordanian legislature's plan.

Thus, cybercrimes can be defined in two ways. The first definition focuses on the means of committing the crime, whereas any crime committed using any electronic or digital device or using any means of communication on the computer network or information technology is a cybercrime. For example, online fraud is a cybercrime in which the criminal uses the computer or the smartphone to access the internet and communicate with the victim to perform the criminal act. The second definition focuses on the object and place of the crime. For instance, if electronic violations are committed on data, information systems, websites, internal networks, contents of computers, storage disks, or any digital or non-digital device containing data or information then it is also considered a cybercrime.

Hence, it is difficult to limit the definition of cybercrime to a specific and comprehensive one given the wide application of such crimes and the evolution of information technology, which constantly creates new electronic and technological means. In order to overcome this issue, most of the legislation, including the Cybercrimes Law in Jordan (Cite to Cybercrime Law, 27 C.F.R., 2015), have provided examples of cybercrimes and included these acts in their international conventions such as illegal access to information systems and data, theft, modification, destruction, alteration, obstruction of access, withholding, and concealment.

3.5.2. Characteristics of cybercrimes

Prior research indicates that cybercrimes have a unique nature that distinguishes them from traditional crimes because they are linked to information systems, computers, and data and are more likely to be committed by a more knowledgeable criminal than the traditional criminal as cybercriminals use or target modern technology (Kshetri, 2010a, 2010b). Thus, the characteristics of cybercrimes include:

1. The technological element is one of the most critical features of cybercrimes. Thus technology, can be the means or place of committing the crime. It is therefore of a technical nature.
2. It is not easy to detect and prove cybercrimes. This crime is characterized by a lack of acquired cases compared to traditional crimes due to its technical nature, which may often involve some complexity or the reluctance of some companies and service providers to report such crimes to maintain confidentiality of the customers. Furthermore, cybercrimes have no tangible physical impact because they focus on information systems where the evidence can be easily erased and deleted. Furthermore, people's awareness also varies between different classes of society, where many people may be subjected to attacks on their data and information systems without genuinely knowing that they have been attacked. Hence, the nonphysical evidence of these crimes can be easily concealed and disposed of due to the lack of external impact of these crimes as they are executed through electrical pulses where figures and data can be easily altered and erased. In addition, the offender in this crime is usually not present at the scene but carries out the crime remotely using the internet, leaving no physical evidence of their existence.

Moreover, many devices and servers that contain a memory full of data or are connected to an information network which contains an enormous amount of data and information that individuals cannot review and verify. Therefore, a little conclusive evidence may be lost in these devices, making it challenging to keep and review.

3. The international nature of these crimes is different from traditional ones. Cybercrimes have been closely linked to information systems, the internet, and other modern means of communication. Thus, in nature, they do not have a geographical barrier or a political limit that obscures it from a particular state. Therefore, the impact of cybercrimes extends to the whole world as this characteristic enables criminals to commit a crime in one country and monitor its results in another country across the globe. Hence, the damage may reach the victim wherever they are located.

3.5.3. Cybercrimes and e-learning

Nowadays, with the world's current situation, educational institutions shifted from campus learning into e-learning; hence, the possibility of cyber-attacks has increased. However, little attention in research was addressed to the issue of awareness in the security of e-learning, particularly as most research discusses cybersecurity awareness in general (Venter et al., 2019). (Raheem and Khan, 2020) have emphasized the importance of being aware of cybersecurity at schools and the methods that stakeholders use to promote cybersecurity in addition to the many challenges, such as the lack of expertise, funding, and resources.

(Bele et al., 2014) also emphasized the importance of raising awareness among students to prevent cybercrime in general. They concluded that it is crucial to create a combined effort of key stakeholders to raise awareness. Thus, they have prepared blended learning courses to promote awareness for such issue (Chandarman and Van Niekerk, 2017). discussed the same issue on students at the tertiary level. In contrast, they have tested student's awareness at private tertiary educational institutions about cybercrimes using a questionnaire that tests their knowledge of different terms related to cybersecurity. They concluded that there is an essential need to promote awareness of cybersecurity among their audience.

(Poonia et al., 2012) also discussed the vital role of having cyber ethics in e-learning environments, understanding the risks of harmful and illegal behavior, and learning how to protect ourselves and other internet users from such behavior. It also involves teaching young people who may not realize the potential for harm to themselves and others online.

Previous studies focused on the awareness of students towards cybercrimes in general and did not explore the connection between cybercrimes and their impact on e-learning.

4. Methodology

This research employed quantitative research methods by administering a questionnaire to research participants. The researchers prepared a questionnaire and distributed it to the students of the University of Jordan who are enrolled in the following three courses: Ethics and Human Values, Communication Skills, and National Culture. These courses were chosen because they were conducted electronically, and the content of these courses included many issues related to the subject of the research, meanwhile all students could fill the questionnaire online. Researchers have the authority to distribute the questionnaire to students through the e-learning system (Moodle).

The distribution of the questionnaire and the collection of information were accurate and non-repetitive since the students had their own username and could only fill out the questionnaire once. It was distributed during the second semester of the academic year 2020/2021. The study used analysis software because it fits the requirements of data collection. SPSS analysis software was used for analyzing the data that consisted of 2648 participants. The sample was obtained by random selection and written consent of all research participants was first granted prior to the process of data collection. No reference to research participants is made in this research as all real identities are protected. The arithmetic averages, standard deviations, ratios and frequencies of the responses were calculated to find the degree of awareness of cybercrimes and the legal procedures and penalties related to electronic crimes in e-learning among students from the University of Jordan. Statistics from the completed questionnaires are presented in Table 1 and Figure 1 below.

5. Results and findings

This section provides a presentation of the results of the study, in an attempt to reveal the degree of awareness of students of the University of Jordan regarding electronic crimes related to e-learning and the legal procedures and penalties involved in such crimes. The results answer the research questions, as follows:

5.1. First: results related to the first research question

What is the degree of awareness of students at University of Jordan regarding electronic crimes related to e-learning and its types?

5.2. Second: results related to the second research question

What is the degree of awareness about legal procedures and penalties related to electronic crimes in e-learning among students at the University of Jordan?

To answer this question, the arithmetic averages, standard deviations, ratios and frequencies of the responses of the students at the University of Jordan were calculated regarding their degree of awareness of the legal procedures and penalties involved in electronic crimes in e-learning. The Dichotomous Scale (Yes = 1, No = 0) was used and depending on the foregoing, and the values of the arithmetic averages were calculated according to the following equation (Al-Bdour et al., 2022):

$$\textit{length of leaves} = \frac{1-0}{3} = \frac{1}{3} = 0.33$$

The highest value is subtracted from the lower value of the answer and the alternatives are divided by the number of levels. Therefore, the “Low” score is from 0.0 - 0.33, the “Medium” score is from 0.34 - 0.66, The “High” score is from 0.67 - 1.00. Table 3 shows the results.

Table 1. Characteristics of participants in the questionnaire.

Variable	Category	Count	Percentage
Gender	Male	669	25.3%
	Female	1979	74.7%
	Total	2648	100%
Course	Ethics and Human Values	1636	61.8%
	Communication Skills	325	12.3%
	National Culture	687	25.9%
	Total	2648	100%

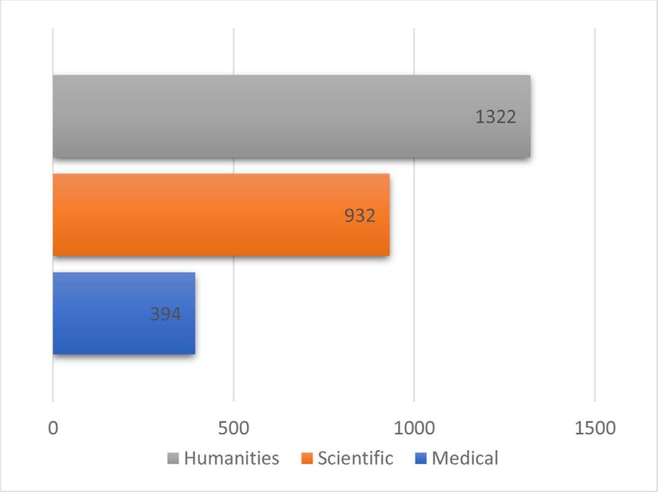

Figure 1. Number of participants according to faculties: Medical, Scientific and Humanities.

Figure 2 shows Arithmetic averages and standard deviations of awareness of e-crimes and legal procedures and penalties related to e-crimes in e-learning.

5.3. Third: results related to the third research question

What are the statistical variations (at the level of significance (α = 0.05)) regarding the degree of awareness of electronic crimes in e-learning among students of the University of Jordan based on study variables (course, gender, and faculty)? To answer this question, the arithmetic averages and standard deviations of the responses of students at the University of Jordan on the awareness of electronic crime related to e-learning were calculated according to the study variables (course, gender, and faculty). A triple analysis of variance was used (Three-Way ANOVA) to find out the significance of the differences, as shown below.

The results in Table 4 indicate that there are apparent differences between the arithmetic averages of the responses of students with respect to the dimensions of awareness of legal procedures and penalties involved with electronic crimes in e-learning according to the variables of the study. To find out the significance of the differences, a three-way analysis of variance was conducted; the results of which are shown in Table 5 below.

5.4. Fourth: results related to the fourth research question

What are the statistical variations (at the level of significance (α = 0.005)) regarding the degree of awareness of legal procedures and penalties related to electronic crimes in e-learning among students of the University of Jordan based on the study variables (course, gender, and faculty)? To answer this question, the arithmetic averages and standard deviations of the responses of students in the dimension of awareness of legal procedures and penalties related to electronic crimes in e-learning were calculated according to the study variables. Three-Way ANOVA was used to determine the significance of the differences, as shown below.

The results in Table 6 indicate that there are apparent differences between the arithmetic averages of the responses of the students of the University of Jordan with respect to the dimension of awareness of legal procedures and penalties related to electronic crimes in e-learning according to the variables of the study. To find out the significance of the differences, a Three-Way analysis was conducted and the results are as shown in Table 7 below.

Table 7 shows that there are statistically significant differences in the dimension of awareness of legal procedures and penalties related to electronic crimes in e-learning according to the variable of course, where

Table 2. Arithmetic averages, standard deviations, and percentages of the responses from participants related to awareness of electronic crimes to e-learning.

Question	Yes	No	Arithmetic average	Standard deviation	Degree
	Percentage				
Do you know what is meant by an electronic crime?	97%	3%	0.97	0.17	High
Is there a difference between an electronic crime and a traditional crime?	83.80%	16.20%	0.84	0.37	High
Have you ever been a victim of electronic crimes?	15.40%	84.60%	0.15	0.36	Low
Which of the following activities is considered an electronic crime related to e-learning?					
Entering an electronic learning system as a teacher or as another student	79.80%	20.20%	0.8	0.4	High
Entering a course that I am not registered in, but that appeared on my e-learning page	28.90%	71.10%	0.29	0.45	Low
Entering course lectures despite the fact that I withdrew from that course	33.80%	66.20%	0.34	0.47	Medium
Recording a lecture without the permission of the course instructor	60.30%	39.70%	0.6	0.49	Medium
Uploading a lecture that was pre-recorded by the course instructor and then publishing it online	51.20%	48.80%	0.51	0.5	Medium
Publishing portions of a recorded lecture	47.10%	52.90%	0.47	0.5	Medium
The use of contents of an educational material on the e-learning website for commercial purposes	76.90%	23.10%	0.77	0.42	High
Recording or taking photos of an exam screen during the exam	75.20%	24.80%	0.75	0.43	High
Taking screenshots of the exam after it has been completed and then publishing them	35.20%	64.80%	0.35	0.48	Medium
Copying announcements from the course page then publishing them	30.30%	69.70%	0.3	0.46	Low
Sending exam links via social media platforms or any other means of communication	26.70%	73.30%	0.27	0.44	Low
Creating a meeting on the e-learning website without the permission of the course instructor	44.40%	55.60%	0.44	0.5	Medium
The use of your colleagues login information to access their accounts on e-learning without their permission only to see their information without changing any content	79.80%	20.20%	0.8	0.4	High
Sitting for a remote exam on behalf of a colleague	76.90%	23.10%	0.77	0.42	High
Asking a specific website to answer the exam questions on your behalf	77.80%	22.20%	0.78	0.42	High
Attempting to break into or hack the system by using special software	84.30%	15.70%	0.84	0.36	High
The use of the exam system and entering exams that is not designated for you	62.60%	37.40%	0.63	0.48	Medium
Entering a course page or course group that is not registered in your course schedule with the intention of obtaining passwords or a link to the lecture	69%	31%	0.69	0.46	High
Entering a course page or course group that is not registered in your academic schedule	58.20%	41.80%	0.58	0.49	Medium
Muting or disabling audio from your colleagues or the lecturer while the synchronous lecture is in progress	71.10%	28.90%	0.71	0.45	High
Sending a large number of messages that are not related to the educational material through the course page or group	44.40%	55.60%	0.44	0.5	Medium
Sending malicious software or harmful programs via a course page or group	81.20%	18.80%	0.81	0.38	High
Sending several questions about the course material through the course page or group	20.20%	79.80%	0.2	0.4	Low
Entering the pages of the learning management systems and posting offensive comments against one of your colleagues or the course instructor	81.10%	18.90%	0.81	0.39	High
Entering the pages of the learning management systems and posting some phrases that may be insinuating hatred against your colleagues or the course instructor	79%	21.00%	0.79	0.41	High
Creating an email, or page, or group using the name of the course	45.10%	54.90%	0.45	0.5	Medium
Creating an email on behalf of one of your colleagues with the intent to communicate with the instructor on his/her behalf	79.40%	20.60%	0.79	0.4	High
Creating an email with the instructors name to correspond with students so as to ensure that students communicate with you	79.20%	20.80%	0.79	0.41	High
The extent of awareness of e-crimes related to e-learning			0.61	0.23	Medium

Table 3. Arithmetic averages, standard deviations, and percentages of the responses of participants related to awareness of legal procedures and penalties involved in electronic crimes in e-learning.

Question	Yes	No	Arithmetic Average	Standard Deviation	Degree
	Percentage				
I believe that an electronic crime is only a hypothetical crime (which has no basis in reality)	14.7%	85.3%	0.85	0.35	High
Does Jordanian Electronic crime law include electronic crimes related to e-learning?	50.5%	49.5%	0.50	0.50	Medium
Do you think that the regulations and laws at the University of Jordan (such as the code of conduct or student discipline system, …etc.) include electronic crimes in e-learning?	57.9%	42.1%	0.58	0.49	Medium
Do you think that there are deterrent penalties for those who commit electronic crimes in e-learning?	67.7%	32.3%	0.68	0.47	High
Do you think it is necessary to file a complaint with the legal authorities when exposed to electronic crimes in e-learning within the University of Jordan?	82.9%	17.1%	0.83	0.38	High
Are there legal procedures to file a complaint when you are exposed to an electronic crime in e-learning within the university?	53.2%	46.8%	0.53	0.50	Medium
Are there legal procedures to file a complaint against someone who commits an electronic crime in e-learning within the university or with the competent judicial authorities?	56.4%	43.6%	0.56	0.50	Medium
The extent of awareness of e-crimes related to e-learning			0.65	0.28	Medium

the value of (P) reached (14.375) at a level of significance of (.000). The table also shows the presence of statistically significant differences according to the gender variable, where the value of (P) reached (12.871) at the level of significance (.000). The arithmetic mean of male student participants was less than that of the female ones. The table also shows no statistically significant differences according to the variable of faculty, where the value of (P) was (0.671) at the level of significance of (0.511), which is a non-statistically significant value.

In order to find out the source of the differences in student's responses on the dimension of awareness of legal procedures and penalties related to electronic crimes in e-learning according to the course variable, Scheffe's test was conducted for dimensional comparisons. Table 8 below presents the results.

6. Discussion

First: What is the degree of awareness of students at University of Jordan regarding electronic crimes related to e-learning and its types?

Table 2 shows that the arithmetic mean of the dimension of awareness of electronic crimes related to e-learning was average with an arithmetic mean of (0.61) and a standard deviation of (0.23). When the students were asked, “Do you know what is meant by electronic crime?” The arithmetic mean of their responses was (0.97) to a high degree. When asked, “Is there a difference between an electronic crime and a traditional crime?” The arithmetic mean of their responses was (0.84) to a high degree, and to the question, “Have you ever been a victim of electronic crimes?” The arithmetic mean of their responses was (0.15), which is a low score. Moreover, when asked “Which of the following activities is considered an electronic crime related to e-learning?” The sub-question that states “Attempting to break into or hack the system by using special software” ranked first with an average of (0.84), which is a high degree, while ranking in second place was the sub-question “Sending malicious software or harmful programs via a course page or group” with an average of (0.81), which is also a high degree.

The sub-question that states “Sending exam links via social media platforms or any other means of communication” ranked penultimate with an arithmetic average of (0.27), which is a low degree, and the sub-question “Sending several questions about the course material through the course page or group” ranked last with an arithmetic average of (0.20), which is also a low degree.

Students' degree of awareness of cybercrimes was high. Because students use the internet extensively as part of their daily routine, they know what cybercrimes mean and can differentiate it from traditional ones. Therefore, students deal with it carefully, and the fact that the student committees at the University of Jordan constantly spread awareness among students of the dangers of exposure to cybercrime indicates the efforts made by competent authorities in spreading awareness of the risks of exposure to cybercrime.

Second: What is the degree of awareness among students at the University of Jordan about legal procedures and penalties related to electronic crimes in e-learning?

Table 3 shows that the arithmetic mean of the dimension of awareness of legal procedures and penalties related to electronic crime was average, with an arithmetic mean of (0.65) and a standard deviation of (0.28). The statement “I believe that an electronic crime is only a hypothetical crime (which has no basis in reality)” ranked first with a mean score of (0.85), which is a high degree, and the statement “Do you think it is necessary to file a complaint with the legal authorities when exposed to electronic crimes in e-learning within the University of Jordan?” ranked second with a high arithmetic average (0.83). The statement “Does the Jordanian Electronic Crime Law include electronic crimes related to e-learning?” ranked last with an arithmetic mean (0.50), which is a medium degree.

The answer to the second question, about the degree of awareness among students of the University of Jordan about legal procedures and penalties related to electronic crimes in e-learning was medium. This indicates the students' lack of awareness of the effectiveness of procedures and penalties for electronic crimes that can be applied in e-learning due to the rapid transition in the learning process at the University of Jordan from traditional learning to distance e-learning that was imposed during the Corona pandemic period, so it did not give sufficient time to clarify procedures and penalties of cybercrime-related to e-learning. Therefore, it was necessary to increase the procedures for spreading awareness of the use of e-learning responsibly, educate students at the University of Jordan about the damages resulting from these electronic crimes, and present the foundations of legal accountability if the student commits an electronic crime related to e-learning.

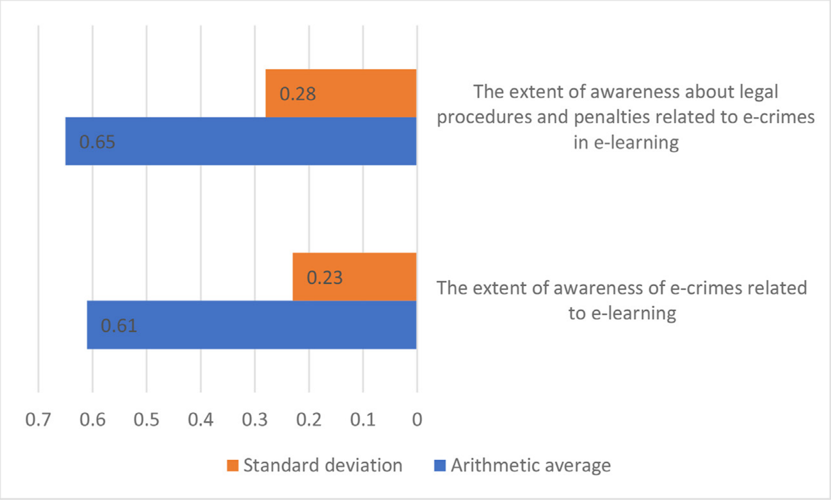

Figure 2. Arithmetic averages and standard deviations of awareness of e-crimes, legal procedures and penalties related to e-crimes in e-learning.

Table 4. Arithmetic averages and standard deviations of the responses of participants according to the study variables.

Variable	Category	Count	Arithmetic Average	Standard Deviation
Course	Ethics and Human Values	1636	0.60	0.23
	Communication Skills	325	0.61	0.22
	National Culture	687	0.61	0.22
Gender	Male	669	0.59	0.24
	Female	1979	0.61	0.23
Faculty	Medical	394	0.63	0.20
	Scientific	932	0.60	0.23
	Humanities	1322	0.60	0.24

Table 5. Results of the Three-way ANOVA test regarding the dimension of awareness of electronic crime related to e-learning according to the study variables.

Contrast Source	Sum of the Squares	Degree of Freedom	Mean of Squares	Value of (f)	Significance Level
Course	0.014	2	0.007	0.129	0.879
Gender	0.178	1	0.178	3.364	0.067
Faculty	0.298	2	0.149	2.825	0.059
Error	139.464	2642	0.053		
Total Average	139.995	2647			

*Level of Statistical Significance (α = 0.05).

Third: What are the statistical variations (at the level of significance (α = 0.05)) regarding the degree of awareness of electronic crimes in e-learning among the students of the University of Jordan based on study variables (course, gender, and faculty)?

Table 5 shows that there are no statistically significant differences in the dimension of awareness of legal procedures and penalties related to electronic crimes in e-learning according to the variable of course, where the value of (F) was (0.129) at the level of significance (0.879). The table also shows that there are no statistically significant differences according to the gender variable, where the value of (F) was (3.364) at the level of significance (0.067). The table also shows that there are no statistically significant differences according to the variable of faculty, such that the

Table 6. Arithmetic averages and standard deviations of the responses of participants regarding awareness of legal procedures and penalties related to electronic crimes in e-learning according to the study variable.

Variable	Category	Count	Arithmetic Average	Standard Deviation
Course	Ethics and Human Values	1636	0.67	0.28
	Communication Sills	325	0.58	0.30
	National Culture	687	0.64	0.27
Gender	Male	669	0.62	0.30
	Female	1979	0.66	0.28
Faculty	Medical	394	0.65	0.27
	Scientific	932	0.65	0.28
	Humanities	1322	0.65	0.29

Table 7. Results of the Three-Way ANOVA test related to electronic crimes in e-learning according to the faculty variable.

Contrast Source	Sum of Squares	Degree of Freedom	Mean of Squares	Value of (P)	Level of Significance
Course	2.349	2	1.174	14.735	0.000*
Gender	1.026	1	1.026	12.871	0.000*
Faculty	0.107	2	0.053	0.671	0.511
Error	210.572	2642	0.080		
Total Average	213.956	2647			

*Level of Statistical Significance (α = 0.05).

Table 8. Scheffe's Test for the dimension of awareness of legal procedures and penalties related to electronic crimes in e-learning according to the course variable.

Secondary School Tract		Difference between means (I-J)	Significance
I	J		
Ethics and Human Values	Communication Skills	.0901*	0.000
Ethics and Human Values	National Culture	0.0295	0.072
Communication Skills	National Culture	-.0606-*	0.006

*Level of Statistical Significance (α = 0.05).

value of (F) was (2.825) at the level of significance (0.059), which is a non-statistically significant value.

The answer to the third question about the degree of commitment of students to patterns of ethical behavior in e-learning was high. This indicates students' interest in synchronous and asynchronous meetings and teaching activities carried out by faculty members using active learning and critical and creative thinking methods, which contributes to the student's observance of communication etiquette and interest in solving activities and duties. No differences appeared based on the variable of the subject for the similarity of teaching methods among faculty members in e-learning, and no differences appeared based on the variable of gender for the interest of students, whether male or female, in awareness of cybercrimes related to e-learning and because of the similarity of levels of awareness between males and females, in all disciplines and faculties of the University of Jordan.

These results indicate the efforts made by the official authorities at the University of Jordan through their keenness to provide awareness of the dangers of cybercrime through a partnership with the Cybercrime Unit of the Criminal Investigation at the Public Security Directorate by giving awareness lectures at the University of Jordan and through their continuous cooperation with its students in general.

Fourth: What are the statistical variations (at the level of significance (α = 0.005)) regarding the degree of awareness of legal procedures and penalties related to electronic crimes in e-learning among students of the University of Jordan based on the study variables (course, gender, and faculty)?

Table 8 shows that there are significant differences at the level (α = 0.05) regarding the dimension of awareness of legal procedures and penalties related to electronic crimes in e-learning between students of the Communication Skills course, students of the Ethics and Human Values course, and those of the National Culture course. The arithmetic mean of responses of students of the Communication Skills course was less than the arithmetic average of the responses of the students of the Ethics and Human Values, and National Culture courses. However, there were no statistically significant differences between the students of the courses of Ethics and Human Values and the National Culture.

As for the answer to the fourth question, which indicated the degree of awareness of legal procedures and penalties related to electronic crimes in e-learning among Jordanian University students based on the study variables (course, gender, and college), female students were more interested than male students in the degree of awareness of legal procedures and penalties related to electronic crimes in e-learning. This is due to the interest and keenness of families to educate their children about the dangers of cybercrime, and the responsible use of the internet. Students' responses of ethics and human values, and national culture courses were higher than that of communication skills course, as there are units dedicated to the legal procedures and penalties related to cybercrimes in e-learning, namely through the student's code of conduct at the University of Jordan.

Prior studies focused on students' awareness towards cybercrimes in general or the importance of protecting educational systems from cybercrime, meanwhile they did not explore the connection between cybercrimes and their impact on e-learning. They also did not investigate the degree of students' awareness about cybercrimes related to e-learning. This study attempt to find the degree of students awareness in using e-Learning at the University of Jordan whether the students were cyber-victims or cybercriminals, and to also find the degree of awareness in misuse behavior such as cheating, impersonation, or infringement of intellectual property rights whether they consider it as cybercrimes if they did it using internet.

7. Recommendations

1. After considering the findings of the study, we recommend the following: Amending the texts of the student's code of ethics at the University of Jordan to create new content that contain references to educate students about the effects of cybercrime, where it is possible to identify the images of these cybercrimes and the penalties incurred by the university and ways to prevent them. Because the results in Tables 4 and 5 indicate that there are apparent differences between the arithmetic averages of the responses of students with respect to the dimensions of awareness of legal procedures and penalties involved with electronic crimes in e-learning according to the variables of the study. Table 2 shows that the arithmetic means of the dimension of awareness of electronic crimes related to some questions is low, meanwhile the discussion for the third and fourth questions indicate that spreading awareness of the risks of exposure to cybercrime through the courses that are taught at the University of Jordan that include information about cybercrime.
2. According to the results related to question one, raising awareness among students, administrators, and faculty members at the University of Jordan about cybercrimes and urging students to interact with the local community to confront crimes in the electronic information environment by holding seminars and workshops within projects for voluntary work.
3. Implementation of several specialized courses in cybercrimes for students, faculty members, and administrators at the University of Jordan to be aware of the nature of these crimes and ways of evading them. To clarify the importance of this point, we may refer to the results and discussion in questions number 1,3,4.
4. Addressing decision-makers in higher education institutions about the need to develop legislation related to electronic crimes in education. The course plans of undergraduate and postgraduate programs must be modified to include specialized courses in cybercrimes. In addition to the above, materials specialized in cybercrimes must be added to the pre-university education curriculum to reinforce cybercrime awareness within Jordan's local community. In this issue referring to the results and discussion in questions number 1,2,3,4 is very important.
5. The University of Jordan's faculties can cooperate with the Cybercrime Unit in the Public Security Directorate to establish technical teams to collect evidence in cybercrime cases. This collaboration will provide the local community in Jordan with the competencies and expertise necessary to work on the existence of a national strategy to raise awareness of cybercrime that guides individuals to avoid falling into cybercrime. The results related to question number three shows the ethical behavior in e-learning was high because of meetings and teaching activities carried out by faculty members using active learning and critical and creative thinking methods.
6. Developing e-learning software and tools and making use of artificial intelligence to reduce electronic crimes. The results belong to the four questions (1,2,3,4).
7. Issuing periodic bulletins by higher education institutions regarding awareness of the dangers and violations in cybersecurity, on the condition that it addresses all that is new in this field. The results belong to the four questions (1,2,3,4).
8. Conducting more studies that deal with electronic crime issues in education to learn more about the risks and violations, especially in light of the need to develop e-learning systems. This point is mainly related to the results in questions number (3,4).

8. Limitations and future scope

A limitation of this research is that only one university was considered in Jordan. For future work we are interested in conducting the same study on different universities in Jordan in order to generalize the results of the study.

9. Conclusion

In this study, we explored the degree of awareness, among students at the University of Jordan about cybercrimes related to e-learning and the legal procedures and penalties related to electronic crimes in e-learning. To this end, quantitative research methods were used, by distributing a questionnaire to (2,648) students who were enrolled in three online courses. The findings suggest that the students had a high awareness about cybercrime, and the degree of students' awareness in the University of Jordan about legal procedures and penalties related to electronic crimes in e-learning was medium. These findings are significant due to the widespread use of the internet by students as part of their daily routine and after the COVID-19 pandemic when learning in universities and schools was transferred online. Based on these findings, the study presented a set of recommendations that can be used to increase awareness and maximize the benefit of using e-learning.

Declarations

Author contribution statement

Hani Y. Ayyoub; Ahmad A. AlAhmad: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Amani Al-Serhan; Mohammad F. Al-Abdallat: Conceived and designed the experiments; Performed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Esra'a Al-Muheisen; Hadeel Boshmaf; Yasmeen A. Abu-Taleb; Yarob O. Alqudah; Yazan Alshamaileh: Conceived and designed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data availability statement

Data will be made available on request.

Declaration of interest's statement

The authors declare no conflict of interest.

Additional information

Supplementary content related to this article has been published online at https://doi.org/10.1016/j.heliyon.2022.e10897.

References

Adams, A., Blanford, A., 2003. Security and Online Learning: to Protect and Prohibit. In: Usability Evaluation of Online Learning Programs. IGI Global, pp. 331–359.

Adnan, M., Anwar, K.J.O.S., 2020. Online learning amid the COVID-19 pandemic: students' perspectives. Online Submission 2 (1), 45–51.

Al-Bdour, M., AlShawabkeh, M.a., Alni'mat, A., AlRyalat, S.A., Abuameerh, O., 2022. Students' perceptions of e-learning in medical faculties in Jordan during the COVID-19 pandemic. Int. Med. J. 29 (2).

Algahtani, A., 2011. Evaluating the Effectiveness of the E-Learning Experience in Some Universities in Saudi Arabia from Male Students' Perceptions. Durham University.

Almosa, A., 2002. Use of Computer in Education. Future Education Library, Riyadh, Saudi Arabia.

Almosa, A., Almubarak, A., 2005. E-Learning Foundations and Applications. Riyadh, Saudi Arabia.

Alsoud, A.R., Harasis, A.A., 2021. The impact of covid-19 pandemic on student's e-learning experience in Jordan. J. Theor. Applied Electr. Comm. Res. 16 (5), 1404–1414.

Alwi, N.H.M., Fan, I.-S., 2010. E-learning and information security management. International Journal of Digital Society 1 (2), 148–156.

Arkorful, V., Abaidoo, N., 2015. The role of e-learning, advantages and disadvantages of its adoption in higher education. Int. J. Instr. Technol. Dist. Learning 12 (1), 29–42.

Aydın, C.H., Tasci, D., Society, 2005. Measuring readiness for e-learning: reflections from an emerging country. J. Educ. Technol. 8 (4), 244–257.

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., Zarsky, T., 2007. Cybercrime: Digital Cops in a Networked Environment, 4. NYU Press.

Barakat, M., Farha, R.A., Muflih, S., Ala'a, B., Othman, B., Allozi, Y., Fino, L., 2022. The era of E-learning from the perspectives of Jordanian medical students: a cross-sectional study. Heliyon 8 (7).

Bele, J.L., Dimc, M., Rozman, D., Jemec, A.S., 2014. Raising Awareness of Cybercrime–The Use of Education as a Means of Prevention and Protection. ERIC.

Borotis, S., Poulymenakou, A., 2004. E-learning readiness components: key issues to consider before adopting e-learning interventions. In: Paper Presented at the E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education.

Campbell, L., 2004. What does the "e" stand for. Department of Science Mathematics Education. The University of Melbourne, Melbourne.

Carlisle, L., 2020. Investing in E-Learning Remains a Priority for UNHCR Jordan. Retrieved from. https://www.unhcr.org/jo/13661-investing-in-e-learning-remains-a-priority-for-unhcr-jordan.html.

Chandarman, R., Van Niekerk, B., 2017. Students' cybersecurity awareness at a private tertiary educational institution. The African J. Inform. Communication 20, 133–155.

Crawford, J., Butler-Henderson, K., Rudolph, J., Malkawi, B., Glowatz, M., Burton, R., Lam, S., 2020. COVID-19: 20 countries' higher education intra-period digital pedagogy responses. Journal of Applied Learning Teaching 3 (1), 1–20.

Cybercrime Law, 27 C.F.R. (2015).

Fawaz, M., Samaha, A., 2021. E-learning: Depression, Anxiety, and Stress Symptomatology Among Lebanese university Students during COVID-19 Quarantine. In: Paper Presented at the Nursing Forum.

Gandhi, V.K., Thanjavur, T.N.S.I., 2012. An overview study on cyber crimes in internet. J. Inf. Eng. Appl. 2 (1), 1–5.

Gonzalez, T., De La Rubia, M., Hincz, K.P., Comas-Lopez, M., Subirats, L., Fort, S., Sacha, G., 2020. Influence of COVID-19 confinement on students' performance in higher education. PLoS One 15 (10), e0239490.

Keller, C., Cernerud, L., 2002. Students' perceptions of e-learning in university education. J. Educ. Media 27 (1-2), 55–67.

Kerr, O.S., 2003. Cybercrime's scope: interpreting access and authorization in computer misuse statutes. NYUL Rev 78, 1596.

Kidd, T.T., 2009. Online Education and Adult Learning: New Frontiers for Teaching Practices: New Frontiers for Teaching Practices. IGI Global.

King, C.G., Guyette Jr., R.W., Piotrowski, C., 2009. Online exams and cheating: an empirical analysis of business students' views. J. Educ. Online 6 (1), n1.

Kshetri, N., 2010a. Cloud computing in developing economies. Computer 43 (10), 47–55.

Kshetri, N., 2010b. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Springer Science & Business Media.

Kunz, M., Wilson, P., 2004. Computer Crime and Computer Fraud. Retrieved from.

LaRose, R., Gregg, J., Eastin, M., 1998. Audiographic telecourses for the Web: an experiment. J. Computer-Mediated Commun. 4 (2), JCMC423.

Lewis, J.R., 2018. Is the report of the death of the construct of usability an exaggeration? J. Usability Studies 14 (1), 1–7.

Liguori, E., Winkler, C., 2020. From Offline to Online: Challenges and Opportunities for Entrepreneurship Education Following the COVID-19 Pandemic. In: Entrepreneurship Education Pedagogy, 3. SAGE Publications Sage CA, Los Angeles, CA, pp. 346–351.

Mailizar, A., Abdulsalam, M., Suci, B., 2020. Secondary school mathematics teachers' views on e-learning implementation barriers during the COVID-19 pandemic: the case of Indonesia. Eurasia J. Math. Sci. Technol. Educ. 1–9.

Maimon, D., Louderback, E.R., 2019. Cyber-dependent crimes: an interdisciplinary review. Annual Review of Criminology 2, 191–216.

Marino, T., Eager, M., Draxler, T., 2000. Learning Online: A View from Both Sides. The National Teaching & Learning Forum. Paper presented at the.

Ndume, V., Tilya, F., Twaakyondo, H., 2008. Challenges of adaptive elearning at higher learning institutions: a case study in Tanzania. Int. J. Comput. Intell. Res. 2 (1), 47–59.

Petee, T.A., Corzine, J., Huff-Corzine, L., Clifford, J., Weaver, G., 2010. Defining "cyber-crime": issues in determining the nature and scope of computer-related offenses. Futures Working Group 5, 6–11.

Poonia, A.S., Dangayach, G., Bhardwaj, A., 2012. Integrating and teaching cyber ethics in eLearning environment. Int. J. Comput. Integrated Manuf. 20, 1–6.

Raheem, B.R., Khan, M.A., 2020. The role of e-Learning in COVID-19 crisis. Int. J. Creat. Res. Thoughts 8 (3), 3135–3138.

Reeves, T.C., 2000. Alternative assessment approaches for online learning environments in higher education. J. Educ. Comput. Res. 23 (1), 101–111.

Rogers, C.F., 2006. Faculty perceptions about e-cheating during online testing. J. Comput. Sci. Colleges 22 (2), 206–212.

Rossi, P., 2009. Learning environment with artificial intelligence elements. J. e Learn. Knowl. Soc. 5 (1), 67–75.

Rowe, N.C., 2004. Cheating in online student assessment: beyond plagiarism. Online J. Dist. Learn. Adm. 7 (2).

Salahshouri, A., Eslami, K., Boostani, H., Zahiri, M., Jahani, S., Arjmand, R., Dehaghi, B.F., 2022. The university students' viewpoints on e-learning system during COVID-19 pandemic: the case of Iran. Heliyon 8 (2), e08984.

Shahroury, F.R., 2022. E-LEARNING during COVID-19 epidemic: experience of a university from Jordan. Acad. Strat. Manag. J. 21 (S4).

Srivastava, A., Sinha, S., 2013. Information security through e-learning using VTE. Int. J. Electron. Comput. Sci. Eng. 2 (18), 528–531.

Toquero, C.M., 2020. Challenges and opportunities for higher education amid the COVID-19 pandemic: the Philippine context. Pedagogical Res. 5 (4).

Underwood, J., Szabo, A., 2003. Academic offences and e-learning: individual propensities in cheating. Br. J. Educ. Technol. 34 (4), 467–477.

Urdan, T.A., Weggen, C.C., 2000. Corporate Elearning: Exploring a New Frontier.

Venter, I.M., Blignaut, R.J., Renaud, K., Venter, M.A., 2019. Cyber security education is as essential as "the three R's". Heliyon 5 (12), e02855.

Watkins, R., Leigh, D., Triner, D., 2004. Assessing readiness for e-learning. Perform. Improv. Q. 17 (4), 66–79.

Wentling, T., Waight, C., Gallaher, J., Fleur, J., Wang, C., Kanfer, A., 2000. E-Learning: A Review of Literature'Knowledge and Learning Systems Group. National Center for Supercomputing Applications, University of Illinois, pp. 1–73.

Zeitoun, H., 2008. E-learning: concept, issues, application, evaluation. In: Riyadh. Dar Alsolateah Publication.

Zhong, R., 2020. The Coronavirus Exposes Education's Digital divide, 18. The New York Times.