DOI: 10.2478/orga-2025-0006

The Impact of Students' Cybersecurity Vulnerability Behavior on E-Learning Obstacles

Ibrahim Mohamed TAHA[1], Rajaa Hussein Abd ALI[2], Ali Abdulhassan ABBAS[3]

[1] Sadat Academy for Management Sciences, Tanta, Egypt, ibrahimaboalazm@gmail.com

[2] University of AL-Zahraa for Women/ College of Health and medical Techniques/ Radiological Technics Department, Kerbala, Iraq, rajaa.ali@uokerbala.edu.iq, ms.rajaahussien@gmail.com

[3] University of Kerbala, College of Administration and Economics, Department of Accounting, Kerbala, Iraq, fuhrer313@gmail.com, ali.abd.alhassan@uokerbala.edu.iq

Background/purpose: This study examines the relationship between students' cybersecurity vulnerability behavior and e-learning obstacles. With the rapid growth of online education, ensuring the security and privacy of digital platforms has become crucial. In this background, the current study is a first-of-its-kind attempt to understand the relationship between these two variables in the background of higher educational institutions in Iraq.
Methods: For this study, the researchers collected data during 2023 from students aged between 19 and 25 enrolled in the University of Karbala, Iraq, using a semi-structured research questionnaire, who were selected through a random sampling method. The questionnaire comprised questions pertaining to the dimensions of both the dependent and the independent variable. A total of 350 valid responses were considered for the analysis in which PLS-SEM was conducted.
Results: The outcomes revealed that the professional and human obstacles have a high association with cybersecurity vulnerability behavior. The study also found that the overall obstacles have a significant effect on the cybersecurity vulnerability behavior. All hypotheses were verified and the outcomes confirm that there is an effective relationship between cybersecurity vulnerability behavior and e-learning obstacles
Conclusion: Based on the study outcomes, the authors proposed a few recommendations for all the stakeholders of the e-learning process, such as educational institutions, governments, faculty members, students, and their parents. Though the current study has been confined to a single university in Iraq, future researchers can focus on expanding the study to other higher educational institutions so that a nationwide policy-level initiative can be brought based on the research evidence.

Keywords: *Cybersecurity Vulnerability Behavior, E-Learning Obstacles, Higher education, PLS-SEM, Student motivation, Learning behaviour*

1 Introduction

E-learning or online learning has become a popular learning method, especially in the aftermath of COVID-19 pandemic (Fauzi, 2022). E-learning brings positive impact on the success of the students in terms of their academics. However, various challenges are associated with e-learning from the perspective of universities/educational institutions (lack of financial and physical resources, lack of technical infrastructure, trained professionals, resistance

Received: 18th March 2024; Accepted: 12th June 2024

from faculty to adopt to novel training methods and so on), students/learners (unable to access internet, lack of necessary equipment/technical infrastructure, high chances of distraction, loss of humanly approach, disconnection with peers and instructors) and the faculty/teacher (access to internet/technical infrastructure, unable to understand the learners' outcomes, clarify their queries etc.,(Mojarad et al., 2023) (Alhamdawee, 2023) mentioned that Iraq opted for e-learning only in the recent years, due to two-decade long political instability, internet unavailability, outdated technical infrastructure, etc., However, Iraqi institutions understood COVID-19 as an opportunity in disguise to upgrade their technical infrastructure and e-learning option by leveraging the open-source and paid platforms like doodle, Google classroom and free conference call etc., In literature, the authors mentioned a variety of challenges in Iraq for e-learning adoption, one of which remains the cybersecurity issue.

Cybersecurity Vulnerability Behavior (CVB) refers to actions or behaviors that increase the chances of experiencing cyber-attack or data breach. In this behavior, the victims tend to lose their confidential data due to their weak passwords or clicking the suspicious links or attachments, failing to update software, or sharing sensitive information (N. F. Khan et al., 2022). When students engage in e-learning platforms, they exhibit cybersecurity vulnerability behavior and expose themselves to cybersecurity risks, including malware, ransomware, or phishing attacks (Wijayanto & Prabowo, 2020).

The impact of students' behavior exposed to cybersecurity on e-learning obstacles can be significant, for instance inability to access the e-learning platforms (Morrow, 2024). In addition to this, a compromised device of the student may be used by the attacker to gain access to the rest of the students and even the platform also. Thus, the cyberattacker may disrupt the module altogether and the institutional infrastructure as well. So, it becomes important to understand the behaviour of the students with regards to cybersecurity risks. Research has shown that a lack of awareness, training, or motivation can contribute to students' cyberattack vulnerability (Vishal Verma & Janardan Pawar, 2024). In the case study published earlier (Al Shabibi & Al-Suqri, 2023), 83% students were found to have been exposed to cybersecurity threats, when they were enrolled in online learning programs during the COVID-19 pandemic. Further, 77% of the target population i.e., post-basic education students from Muscat, lacked awareness about the cybersecurity issues. Therefore, it is important for the educators and administrators to provide the students with appropriate cybersecurity education, training, and resources to reduce the cybersecurity vulnerability behavior and ensure the security and continuity of e-learning activities (Abbas, 2020; Kumar et al., 2022).

E-learning obstacles are of different types such as lecturer-related (desire for change, understanding and knowledge about the technology, sufficient training, technical support etc.,), student-related, curriculum-related and so on (Abeer, 2022). In this background, it is important to understand the relationship between cybersecurity vulnerability behaviour of the students and the e-learning obstacles, since the researchers have mentioned it as a complex phenomenon that requires in-depth understanding (A. H. Ibrahim et al., 2019). Various studies have been conducted earlier focusing cybersecurity awareness among the students and faculty members in Iraq (Abdulla et al., 2023; Al-Janabi & Al-Shourbaji, 2016; Ameen et al., 2017; Nagham Oudeh Alhamdawee, 2023; Tarrad et al., 2022; Zahid et al., 2023), Iraqi private banks (Faez Hasan & Al-Ramadan, 2021), Iraqi national security (Al-Tae et al., 2022), Iraqi organizations (Khadija Hassan & Mustafa Jawad, 2022) and so on. However, there is a lack of studies pertaining to cybersecurity vulnerability behavior and the presence of e-learning obstacles, conducted among students in University of Karbala, Iraq. Thus, the current study is a first-of-its-kind attempt in this domain within the study environment as no other study has been conducted so far, to the best of the authors' knowledge. The current study outcomes will help the decision makers at the institutional level, governments and the cybersecurity organizations that fight the cyberattackers on the daily basis. By understanding the relationship between these two constructs and using a multi-faceted approach, it is important to identify the most vulnerable areas so as to create awareness among students on appropriate cybersecurity practices and provide them with the tools and resources to protect their devices and data.

Based on the study findings, the institutional committees can set up training programs for the students, faculty and other non-teaching staff on how to combat phishing attacks, using safe and complex passwords and making sure the technical infastructure is up-to-date. By promoting good cyber security practices, it is possible for all the stakeholders involved in the e-learning process to reduce the cyberattack vulnerabilities and minimize the impact of their behavior on increasing obstacles to e-learning (Alkaaf, 2023; Arul & Punidha, 2022).

2 Literature review

The current section details about the studies conducted in cybersecurity vulnerability behaviour and the obstacles faced in e-learning system in terms of electronic and physical obstacles, financial and organizational obstacles followed by professional and human obstacles. Cybersecurity vulnerable behavior refers to actions or behaviors that can make an individual, organization, or a system highly vulnerable to cyberattacks or data breaches. Cybersecurity vulnerabilities are weaknesses or gaps in the security measures exploired by the cybercriminals to gain

unauthorized access, steal sensitive data, install malware, or disrupt operations (Ewoh & Vartiainen, 2024).

Poor cybersecurity vulnerability behavior can include a wide range of actions, such as failing to update software and systems, using weak or easy-to-guess passwords, clicking on suspicious links or attachments, sharing sensitive information over unsecured networks or platforms, and neglecting to implement the basic security practices such as two-factor authentication and data backups (Gourisetti et al., 2020). So, it is essential to understand and address the cybersecurity vulnerability behavior to mitigate cybersecurity risks in an effective manner. By identifying and providing a remedy for the vulnerability behavior, both individuals as well as the organizations can reduce the likelihood of successful cyberattacks and protect themselves from potential threats. Some of the studies conducted earlier pertaining to awareness levels among students about cybersecurity have been discussed herewith.

Al-Sherideh (Al-Sherideh et al., 2023) analyzed the satisfaction level of the students enrolled in e-learning platform named Moodle e-learning system, in terms of data security and privacy and their opinions on the overall standard of education. The study outcomes revealed that the presence of security and cybersecurity measures positively influence the increased usage of e-learning modules while the study recommended to get regular feedback and have a constant communication with the students about their experience with the e-learning portals. Thus, it is possible to mitigate the security risks and also have increased engagement. (Bottyan, 2023) assessed the awareness levels among Dunaújváros university students in Hungary, pertaining to cybersecurity using a Personal Cyber Security Provision Scale questionnaire. The questionnaire involved questions regarding protection of privacy, payment information, avoiding the untrusted links, precaution and no trace of transaction history. The study found that password management and performing sensitive transactions on public computers are some of the issues that need to be taken care, since the students are highly exposed to cyberattacks.

Abeer (Abeer, 2022) made an attempt to identify the most important obstacle faced by the lecturers in handling e-learning modules for the purpose of higher education. In this study, the 95 lecturers working in the Palestine Technical University Kadoorie were chosen through convenient sampling method and the outcomes revealed the following challenges in the order of high to low; technological infrastructure > university-oriented > student-related > curriculum-related and finally lecturer-related. The study also established a moderate positive correlation among lecturer, student and the curriculum-bound challenges.

In literature (Abdulla et al., 2023), the authors analyzed the risks involved in data attacks, focusing the University of Sulaimani, Iraq and how far the students and faculty members are aware of social engineering attacks and cyber-security threats. The institution was chosen since the university's internet users invited security risks, confidentiality issues and so on. Using a self-report questionnaire, the data was collected and the outcomes revealed that spear phishing is mostly used by the attackers followed by phishing, baiting, pretexting, quid pro quo and piggybacking, while the victims have significant knowledge about piggybacking. Some of the reasons cited by the participants on not being aware include lack of experience, human error, lack of appropriate training, using same or shared passwords by multiple persons in the same department, not being aware of the social engineering-based attacks, poor knowledge and so on. Cybersecurity vulnerability behaviour includes the following concepts in a broader perspective such as human factors (lack of awareness, training, etc.,), risk management (detection and mitigation of risks followed by risk management practices), threat landscape (constant evolution of threats and the increasing security vulnerabilities), compliance (lack of Standard Operating Procedures and non-adherence to security measures, cybersecurity audits etc) and technology (using outdated software or hardware, absence of technological infrastructure) (Geogiana Buja et al., 2021; Syed, 2020; Yusif & Hafeez-Baig, 2023).

In literature (Tarrad et al., 2022), the authors considered five independent variables such as information security, cybereducation, cyber-training, internet applications and creative behavior with a dependent variable named digital awareness to understand the relationship among these variables and its impact on each other. For this study, 140 school academicians from Eastern Iraq were randomly selected and the data was collected. From the study findings, digital awareness was found to have a positive effect on the rest of the variables. The results emphasized the importance of digital awareness while it urged the government to introduce novel cybersecurity and information security programs within the curriculum itself. In a study conducted among graduate and undergraduate students in Iraq (Zahid et al., 2023), the authors analyzed the impact of demographic features of the individuals upon their awareness levels with regards to cybersecurity. For this study, the authors developed a questionnaire and collected 613 responses. Based on the data analysis outcomes, gender has a significant difference while educational level and age had no significant difference on the cybersecurity awareness. Alzubaidi (Alzubaidi, 2021) measured the awareness level about cybersecurity among 1,230 Saudi Arabian nationals aged above 18 participants, in which the authors assessed the level of awareness and the number of incidents, educational background, critical thinking and the absence of e-government portals for dealing cybercrime-related issues. The study found that half of the participants used personal information to create their passwords while 32.5% had no idea about phishing attacks while 21.7% were already victims of cybercrimes.

3 E-learning obstacles

E-learning has gained wide popularity in recent years, especially after the outbreak of the COVID-19 pandemic. Due to the outbreak, many educational institutions were forced to switch to online learning mode so as to ensure safe distance and avoid public gatherings. E-learning platforms are a flexible, cost-effective, and scalable way to deliver education. However, e-learning model has its own challenges for all the stakeholders involved in the institution such as the decision makers in the institution, technical staff, faculty members, students and their parents (Aborujilah et al., 2022). . The current section details about the studies conducted earlier that defined the issues faced by learners towards e-learning and the ways to address it. In literature (Almaiah et al., 2020), the authors analyzed the critical challenges faced by 30 students, 25 faculty members and 4 e-learning experts at six universities, located in Jordan and Saudi Arabia about the primary factors that support and hinder the adoption of e-learning system. The authors identified the factors that influence the adoption of e-learning and segregated them under various aspects such as trust, system quality, cultural aspects, self-efficacy and interest issues. On the other hand, the challenges found were financial issues, change management conflicts and the lack of technical infrastructure.

Various authors (Barakat et al., 2022; Muhammad, 2022; Pandian, 2023) have summarized the obstacles found in e-learning such as technical issues (low processing capability, faulty or absence of power, hardware and bug issues, compatability etc.,), educational issues (different pedagogical approach, resistance to change from conventional classroom teaching, lack of engagement between the learner and the teacher etc.,), social issues (absence of interaction, less or no motivation, insufficient social skills etc.,), motivational issues and time-management issues. In the systematic review conducted earlier (Mohamed & Kim, 2023), the authors found technology barriers, engagement issues, learning interest among the learners and anxiety to perform are the challenges faced by learners in e-learning programs, enrolled in the educational institutions in Middle east. In the qualitative study conducted among 10 female undergraduate students enrolled in Saudi Public universities (Abed et al., 2022), the authors analyzed how far the learners are motivated and have belief towards online education and the barriers faced by them in terms of societal and religious bases. As per the study findings, the sudden change that occurred during COVID-19 had a heavy impact upon their learning. On the other hand, personal challenges too reduced the student's willingness towards online education.

In a study conducted at Salahaddin University, Iraq, the authors (Ameen et al., 2017) determined the challenges encountered in e-learning and their perceptions about the impact caused by e-learning system in Iraqi higher education. For this study, 300 responses were collected from the students studying in the university through convenience sampling. The findings confirm the following challenges in Iraqi higher educational institutions regarding online learning; inability to get certified, lack of electricity, bad internet connection, absence of a supportive culture and absence of knowledge about the system. Based on the review of literature, it can be understood that there is a lack of studies pertaining to cybersecurity vulnerability behaviour and e-learning obstacles while no study has been conducted at the University of Karbala in this background. In order to fulfil this research gap, the current study aims at understanding the relationship between students' cybersecurity vulnerability behavior and e-learning obstacles.

4 Development of the hypotheses

The current section deals with the development of the hypotheses. Cybersecurity vulnerability behavior refers to actions or inactions that increase an individual's risk of experiencing a cyberattack while such actions include using weak passwords or failing to update software. Learners who use e-learning platforms for engaging in digital learning programs are highly prone to experience cyberattacks. These issues, in turn, can hinder their successful e-learning experience. Additionally, the learners who possess cybersecurity vulnerability behavior are less likely to trust e-learning platforms or feel confident about themselves on using such digital platforms in a safe and effective manner. This lack of confidence and trust can result in motivational issues and hinder their ability to engage with the platform. On this basis, the first main hypothesis has been developed for the study (Abumandour, 2022; Maatuk et al., 2022).

First Hypotheses (H1): *There is a significant relationship between cybersecurity vulnerability behavior and the obstacles to e-learning.*

Based on this main hypothesis, seven sub hypotheses have been framed as briefed herewith. Access to data and information is essential for effective learning in e-learning environments. In the absence of adequate access to data and information, the learning experience becomes incomplete while it also hinders the students from achieving their educational goals. For example, it was found that students perceived access to online resources positively affected their motivation and participation in e-learning (Yeh & Tsai, 2022). Similarly, it was found that insufficient access to data and information was a significant barrier to effective e-learning in healthcare education (Al Shamari, 2022). Moreover, it was found that the lack of access to appropriate resources was one of the major obstacles to the successful adoption of e-learning in the workplace (Abdelfattah et al., 2023). In this background, the first sub-hypothesis has been framed as follows.

The first sub-hypothesis (H1.1): *There is a significant relationship between the Behavior of Data and Informa-*

tion Access and e-learning obstacles.

Access to reliable devices and internet/network connectivity is critical to effective e-learning. Improper device and internet/network use can lead to technical issues, power outages, and limited access to online resources, all of which can affect the student's participation and performance. Therefore, it can be hypothesized that insufficient use of devices and internet/networks may exacerbate these e-learning obstacles, resulting in lower student engagement and performance (M. Khan et al., 2020). It was found that technical issues with hardware and internet/network connectivity were the most significant barriers to effective e-learning during the COVID-19 pandemic (Abeer, 2022). Similarly, it was found that insufficient use of devices and the internet/network were important factors influencing the adoption of e-learning among Jordan and Saudi Arabian university students (Almaiah et al., 2020). Moreover, it found that students with reliable devices and internet/network connections were likelier to engage in e-learning activities. In this background, the second sub-hypothesis has been framed as follows.

The Second sub-hypothesis (H1.2): *There is a significant relationship between the behavior of devices and internet / network usage and e-learning obstacles.*

Using social media can be a distraction for e-learners and can reduce their focus and concentration. Social media addiction can lead to procrastination, poor time management, and lower productivity, affecting student engagement and performance (Vishal Verma & Janardan Pawar, 2024). Therefore, it can be hypothesized that excessive use of social media may exacerbate the obstacles of e-learning, leading to lower student engagement and performance. Several studies have identified the relationship between social media use and e-learning barriers (Abdulhassan Abbas & Hurajah Al Hasnawia, 2020; Sefriani et al., 2023). For example, excessive use of Facebook is associated with lower academic performance among college students (N. T. Khan & Ahmed, 2018).So, was it found that social media addiction was negatively related to academic performance and time management among undergraduate students. Moreover, it was found that the use of social media was a significant predictor of procrastination among college students (Sobaih et al., 2022). In this background, the third hypothesis has been framed as given below.

The third sub-hypothesis (H1.3): *There is a significant relationship between the behavior of social media and e-learning obstacles.*

Password security is an important aspect of eLearning security. Weak or easy-to-guess passwords can result in unauthorized access while the hacked passwords can create a chaos in the e-learning environment, reducing participation (Abeer, 2022; Salman & Shahadab, 2022). Therefore, it can be hypothesized that the behavior of using weak or easy-to-guess passwords may exacerbate e-learning obstacles, leading to lower student engagement and performance Several studies have identified the relationship between password security and e-learning obstacles (Darawsheh et al., 2023; K. Elberkawi et al., 2022; Klaib et al., 2022). For example, a study found that weak passwords were among the most common causes of security breaches in e-learning environments (Khlifi, 2020). Further, it was found that technical issues and accessibility issues were the major obstacles that hinder the adoption of e-learning among adult learners. In this background, the fourth sub-hypothesis has been framed as follows.

The fourth sub-hypothesis (H1.4): *There is a significant relationship between the Behavior of Using Password and e-learning obstacles.*

As mentioned earlier, smartphone addiction can lead to procrastination, poor time management, and lower productivity, affecting student engagement and performance (Peng, 2023; C. Zhang et al., 2022). Several studies have identified the relationship between smartphone use and e-learning obstacles. For example, higher smartphone use levels were associated with lower academic performance among college students. Similarly, it was found that using smartphones for non-academic purposes during class was negatively associated with a student's GPA. Moreover, smartphone addiction was negatively related to academic performance among university students (J. Zhang & Zeng, 2024; Zou et al., 2022). In this background, it can be hypothesized that the excessive use of smartphones may exacerbate these e-learning obstacles, leading to lower student engagement and performance (Sunday et al., 2021). So, the fifth sub-hypothesis has been framed as given below.

The Fifth sub-hypothesis (H1.5): *There is a significant relationship between the behavior of using smartphone devices and e-learning obstacles.*

As mentioned earlier, weak technical infrastructure represented by outdated devices, power outage, lack of access of high-speed internet, networking issues, lack of permanent maintenance, the lack of modern computers, and the lack of original programs remain the most important physical and electronic obstacles towards the widespread adoption of online education. The cybersecurity vulnerability behavior affects this dimension directly based on which the following hypothesis has been developed.

The Six sub-Hypotheses (H1.6): *There is a significant relationship between cybersecurity vulnerability behavior and the electronic and physical obstacles*

In addition to the lack of technical infrastrcutrue, the organizational obstacles such as the lack of financial support, lack of support from the management, lack of equipped and modern scientific laboratories, and the weakness of training programs and so on. These issues tend to have an impact upon the cybersecurity vulnerability behavior based on which the seventh hypothesis has been framed below.

The Seven sub-Hypotheses (H1.7): *There is a significant relationship between cybersecurity vulnerability behavior and financial and organizational obstacles*

The lack of seasoned professionals in the organization, inexperienced faculty members, lack of basic computer education for the students, conventional teaching methods in the field of the internet and computers, the lack of specialized people to maintain devices and update programs, and the absence of clear mechanisms in the employment and application of e-learning heavily affect the Cybersecurity Vulnerability Behavior based on which the eight sub-hypothesis has been framed as given below.

The Seven sub-Hypotheses (H1.8): There is a significant relationship between cybersecurity vulnerability behavior and the professional and human obstacles

5 Methods

In order to achieve the objective, a semi-structured research questionnaire was developed and the number of questions pertaining to each and every dimension of the study are quoted in table 1. Table (1) shows the dimensions of both dependent variable (E-learning obstcles ELO) and the independent variable (Cybersecurity vulnerability behavioru – CVB) used in the current study. The respective number of questions, for the dimensions, used in the questionnaire along with the source articles are shown in the table.

The questionnaire developed was converted into a google form so that the responses can be easily collected and used for analysis. For this study, random sampling method was followed to choose the potential respondents from a pool of students enrolled at the Faculty of Administration and Economics, Department of Accounting, University of Karbala, Iraq. The potential respondents i.e., students were given this questionnaire to respond during the study period 08th May and 19th May 2023. The respondents were given time and informed consent was obtained from the study participants. Out of the total 968 students, 450 students were approached to participate in the study. Based on the responses received and upon validation, 350 valid responses were considered for final analysis. Out of the final responses, 167 (47.71%) were male students and 183 (52.28%) were female students aged between 19 and 25 years. Before completing the design of the study, the researchers conducted interviews among a sample of students in this department, and majority of the respondents reported that they actually encounter numerous obstacles in the field of cybersecurity and also in e-learning, which had an impact on their performance and increased the vulnerability of their accounts to hacking. This study employed the Structural Equation Modeling (SEM) approach with Partial Least Squares as an analytical tool (PLS). PLS studies psychometric traits and provides evidence for the existence or absence of associations (Bagozzi, 1981). SmartPLS 3.2.9 and SPSS 28 were used to analyze the data in this investigation in two phases. The first step measurement model validated the structures' content, convergent, and discriminant validity. In the second step, the structural model and hypotheses were tested. Common Method Bias (CMB) was detected through Harman's single-factor test; the percentage of the factor's explained variance for the common factor (10.8%) was below the threshold of 50%, indicating the absence of this problem (MacKenzie & Podsakoff, 2012).

Table 1: Variable, dimensions and the number of questions pertaining to the dimension in the questionnaire

Variable	Dimensions	number of questions	Type	Source
Cybersecurity Vulnerability Behavior (CVB)	The behavior of Data and Information Access (BDIA)	5	independent	(Wijayanto & Prabowo, 2020)
	The behavior of Device and Internet / Network Usage (BDIU)	4		
	The behavior of social media (BSM)	3		
	The behavior of Using Password (BUP)	5		
	The behavior of Using Smartphone Devices (BUSD)	4		
E-Learning Obstacles (ELO)	Electronic and physical obstacles (EPO)	4	Dependent	(Abeer, 2022; A. F. Ibrahim et al., 2021)
	Financial and organizational obstacles (FOO)	6		
	Professional and human obstacles (PHO)	5		

Table 2: Measurement model assessment

Itmem	BUP	BDIA	BDIU	BSM	BUSD	EPO	PHO	FOO
BUP1	0.401							
BUP2	0.61							
BUP3	0.47							
BUP4	0.467							
BUP5	0.533							
BDIA1		0.57						
BDIA2		0.456						
BDIA3		0.486						
BDIA4		0.663						
BDIA5		0.528						
BDIU1			0.49					
BDIU2			0.716					
BDIU3			0.611					
BDIU4			0.541					
BSM1				0.587				
BSM2				0.585				
BSM3				0.703				
BUSD1					0.533			
BUSD2					0.416			
BUSD3					0.655			
BUSD4					0.595			
EPO1						0.552		
EPO2						0.658		
EPO3						0.595		
EPO4						0.512		
PHO1							0.461	
PHO2							0.652	
PHO3							0.501	
PHO4							0.534	
PHO5							0.66	
PHO6							0.649	
FOO1								0.524
FOO2								0.424
FOO3								0.464
FOO4								0.7
FOO5								0.504
CR	0.622	0.675	0.683	0.659	0.637	0.67	0.751	0.656

6 Results

The current study details about the measurement model for the reflective and latent variables. Further, factor loadings, composite reliability and discriminant validity were also utilized in this study. Further, discriminant validity is assessed through Fornell–Larcker criterion and HTMT ratio. In addition to this, Pearson correlation analysis was conducted after which the structure model was assessed. Finally, the hypothesis testing was conducted and the results are discussed in this section along with discussion.

6.1 Measurement Model

To establish the validity of the model's constructs, the measurement model was evaluated for reflective and latent variables (see Figure 1). Factor loadings, composite reliability (CR), and discriminant validity were used to assess construct validity (Hair et al., 2014). Hair et al. recommended dropping indicators with loading below 0.40 to allow forester composite reliability (CR) (Leguina, 2015) Click or tap here to enter text.. No indicators were dropped from the model, as shown in Table (2) and Figure (1). The values of composite reliability should be greater than 0.6 (Bagozzi, 1981). These indicate that the study satisfied these requirements for convergent validity and internal consistency of the scales.

Further, discriminant validity is assessed through Fornell–Larcker criterion and HTMT ratio. Fornell–Larcker criterion required that each composite AVE square root on the diagonal element be greater than the correlations between the constructs (Leguina, 2015).

The HTMT approach is 'the ratio of the between-trait correlations to the within-traits correlations'. The HTMT values should be lower than 1 (Gaskin et al., 2018). The discriminant validity is established following the previous guides of the Fornell-Larcker criterion and HTMT values in tables 3 and 4.

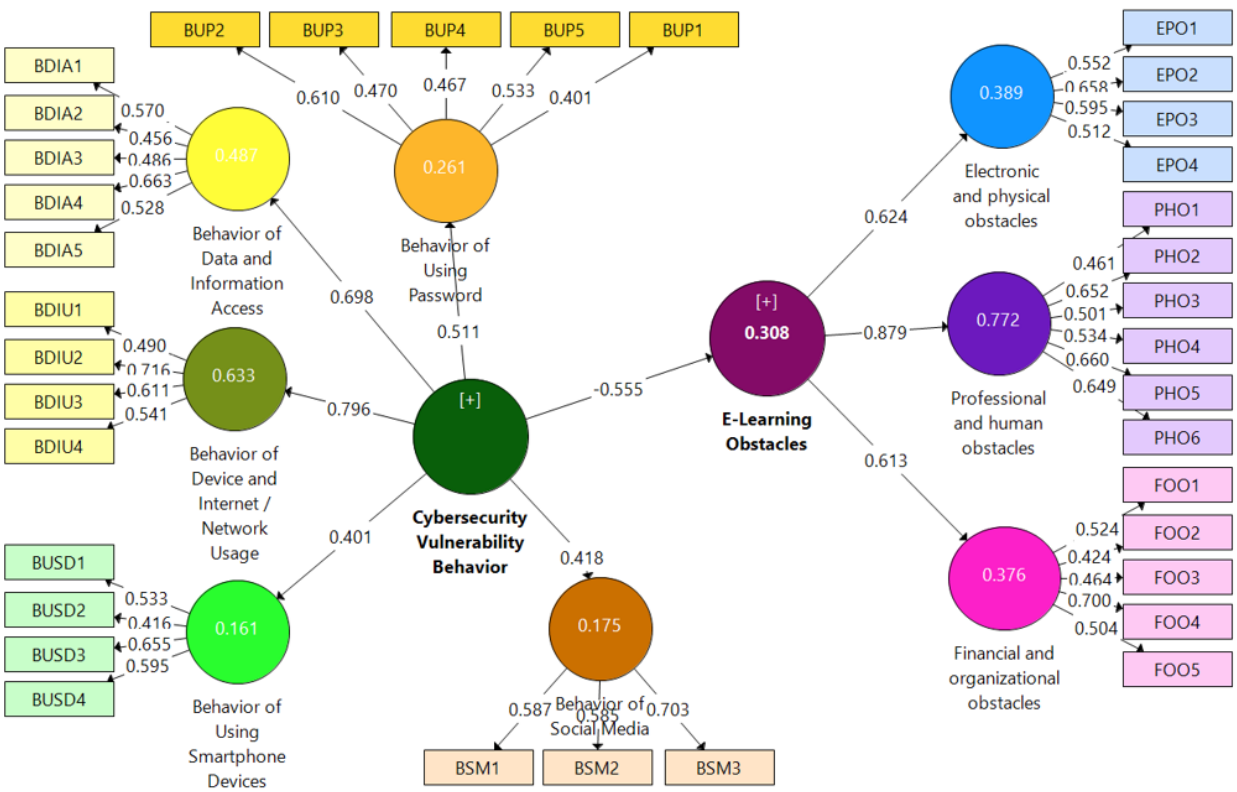

Figure 1: Measurement model assessment

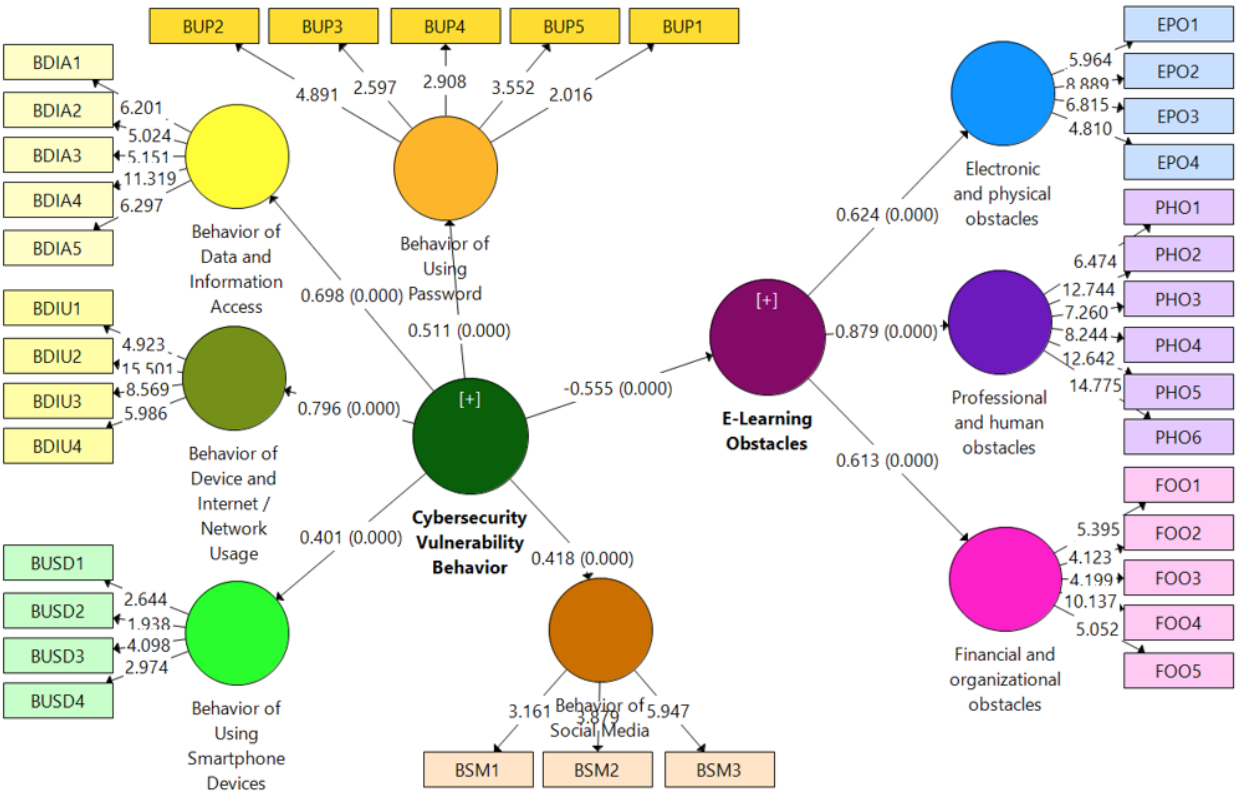

Figure 2: Structural model assessment

Table 3: Discriminant validity (Fornell-Larcker criterion)

	BDIA	BDIU	BSM	BUP	BUSD	EPO	FOO	PHO
BDIA	**0.545**							
BDIU	0.351	**0.596**						
BSM	0.123	0.181	**0.627**					
BUP	0.214	0.213	0.204	**0.501**				
BUSD	0.077	0.28	-0.02	0.069	**0.557**			
EPO	-0.219	-0.352	-0.181	0.069	-0.193	**0.582**		
FOO	-0.117	-0.273	-0.249	0.038	-0.14	0.19	**0.532**	
PHO	-0.388	-0.469	-0.262	-0.123	-0.159	0.328	0.321	**0.582**

Table 4: Discriminant validity (HTMT ratio)

	BDIA	BDIU	BSM	BUP	BUSD	EPO	FOO	PHO
BDIA								
BDIU	0.93							
BSM	0.593	0.713						
BUP	0.733	0.712	0.835					
BUSD	0.618	0.767	0.578	0.631				
EPO	0.685	0.975	0.648	0.643	0.683			
FOO	0.629	0.788	0.98	0.575	0.8	0.656		
PHO	0.72	0.957	0.824	0.494	0.529	0.713	0.673	

Table 5: Descriptive statistics and multiple correlations

		BUP	BDIA	BDIU	BSM	BUSD	EPO	PHO	FOO	CVB	ELO
BUP	**r**	--									
BDIA	**r**	.22***	--								
	P	<.001									
BDIU	**r**	.19***	.32***	--							
	P	<.001	<.001								
BSM	**r**	.20***	.13*	.18***	--						
	P	<.001	0.016	0.001							
BUSD	**r**	0.09	0.06	.26***	-0.03	--					
	P	0.097	0.299	<.001	0.563						
EPO	**r**	0.06	-.20***	-.35***	-.19***	-.17***	--				
	P	0.242	<.001	<.001	<.001	0.001					
PHO	**r**	-.12*	-.34***	-.46***	-.27***	-.16**	.32***	--			
	P	0.030	<.001	<.001	<.001	0.003	<.001				
FOO	**r**	0.02	-0.06	-.23***	-.26***	-0.10	.18***	.31***	--		
	P	0.751	0.252	<.001	<.001	0.057	0.001	<.001			
CVB	**r**	.57***	.58***	.71***	.51***	.49***	-.31***	-.48***	-.23***	--	
	P	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001		
ELO	**r**	-0.02	-.29***	-.4***	-.33***	-.20***	.73***	.76***	.66***	-.48***	--
	P	0.759	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	
M		**3.97**	**3.82**	**4.01**	**3.66**	**3.23**	**3.87**	**3.97**	**3.96**	**3.74**	**3.93**
SD		**0.43**	**0.42**	**0.51**	**0.46**	**0.47**	**0.52**	**0.49**	**0.44**	**0.26**	**0.35**
Skewness		**-0.16**	**0.33**	**-0.17**	**0.31**	**0.41**	**0.19**	**-0.01**	**-0.08**	**-0.43**	**0.24**
Kurtosis		**-0.65**	**-0.06**	**-0.62**	**-0.35**	**-0.10**	**-0.68**	**-0.97**	**-0.62**	**-0.11**	**-0.69**

r= correlation coefficient; P= P-value; M=mean; SD=standard deviation.

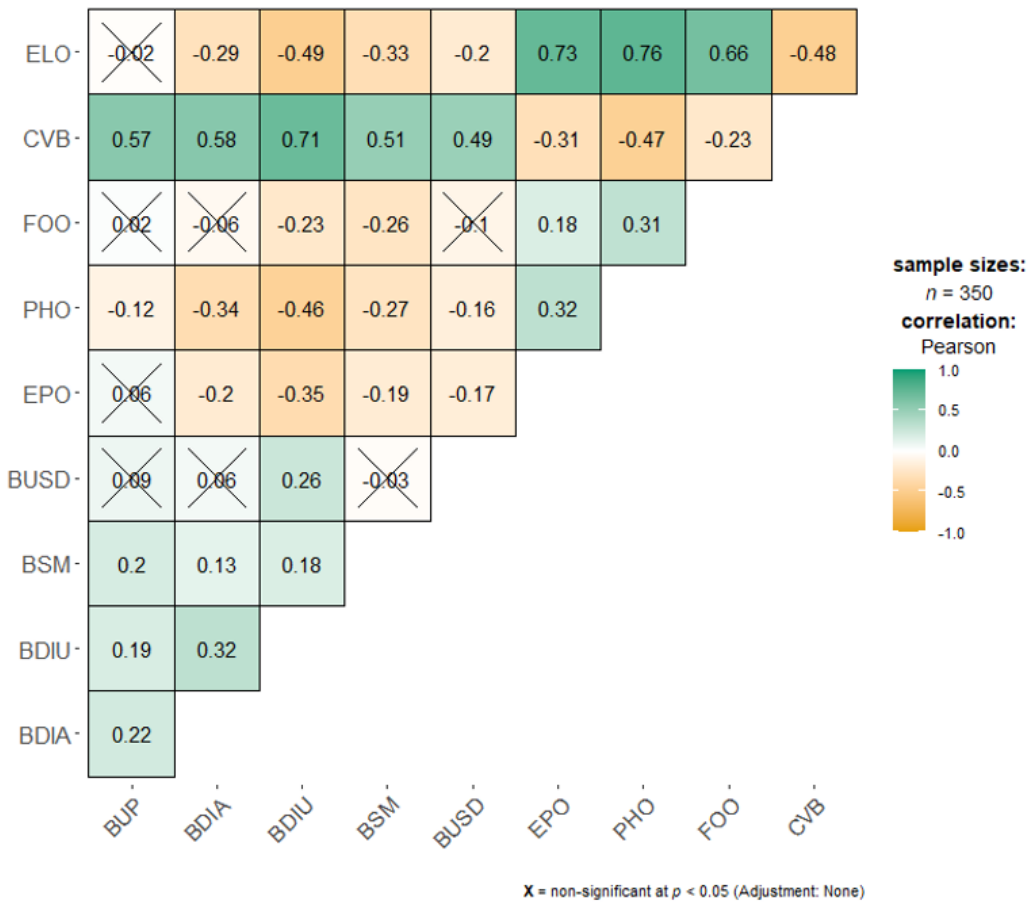

Figure 3: Visualization of the correlation matrix

6.2 Descriptive Statistics and Multiple Correlations

After establishing the reliability and validity of the variables, descriptive statistics and multiple correlations were conducted between the selected constructs including the mean (M) and standard deviation (SD) as shown Table (5). The descriptive statistics for the independent variable "Cybersecurity Vulnerability Behaviour" was (M=3.74,SD=0.26), and for the dependent variable, "E-Learning Obstacles" was (M=3.93,SD=0.35).

Among the dimensions of the independent variable "Cybersecurity Vulnerability Behaviour", it was found that the "BDIU" had the highest mean (M=4.01,SD=0.51) and "BUSD" had the lowest mean (M=3.23,SD=0.47). Among the dimensions of the dependent variable "E-Learning Obstacles", it was found that the "PHO" had the highest mean (M=3.97,SD=0.49) and "EPO" had the lowest mean (M=3.87,SD=0.52). The values for Skewness between -2 to +2 and kurtosis between -7 and +7 are generally considered to be acceptable to prove normal distribution (Byrne, 2016; Hair et al., 2021) Click or tap here to enter text.. The results of the normality test, shown in Table 5, infer that the values of Skewness and kurtosis for the constructs of the model were within the specified range.

Pearson product-moment correlation coefficient is calculated to determine the strength and the direction of the relationship between the selected constructs. Correlation coefficients marked with three stars (***) are significant at 0.001, i.e., 99.9% confidence level; correlation coefficients marked with two stars (**) are significant at 0.01, i.e., 99% confidence level, coefficients marked with one star (*) are significant at 0.05, i.e., 95% confidence level, and finally, coefficients NOT marked are not significant at 0.05, i.e., P-values are greater than 0.05. Table 5 shows the matrix of Pearson correlation coefficients among all the constructs and the dimensions. A negative relationship was found between the independent variable (and its dimensions) and the dependent variable (and its dimensions). However, a significant negative relationship was found between Cy-

bersecurity Vulnerability Behaviour and E-Learning Obstacles since (r(350)=-.48,P<0.001).

6.3 Assessing the Structural Model

Examining the structural model includes path coefficients, collinearity diagnostics, coefficient of determination (R2), effect size (f^2), predictive relevance (Q2), and global goodness of fit criteria. Before analyzing the structural model, the collinearity among the constructs was examined (table 7) using Variance Inflation Factors (VIF), and found that all the values were less than the threshold of 5 (Leguina, 2015).

The results of hypothesis testing in Table 6 and Figure 2 showed that Cybersecurity Vulnerability Behavior yielded a significant negative effect on E-Learning Obstacles since (β=-0.555,t=11.943,P<0.001,95% CI for β=[-0.632,-0.453]), consequently, the first hypothesis is confirmed. Additionally, in Table 5 and Figure 4, the dimensions of Cybersecurity Vulnerability Behavior yielded a significant negative effect on E-Learning Obstacles as follows: Behavior of Data and Information Access (β=-0.214,P<0.001), Behavior of Device and Internet/Network Usage (β=-0.412,P<0.001), Behavior of Social Media (β=-0.258,P<0.001), and Behavior of Using Smartphone Devices (β=-0.147,P=0.001). While Behavior of Using Passwords does not influence E-Learning Obstacles since (β=0.048,P>0.05).

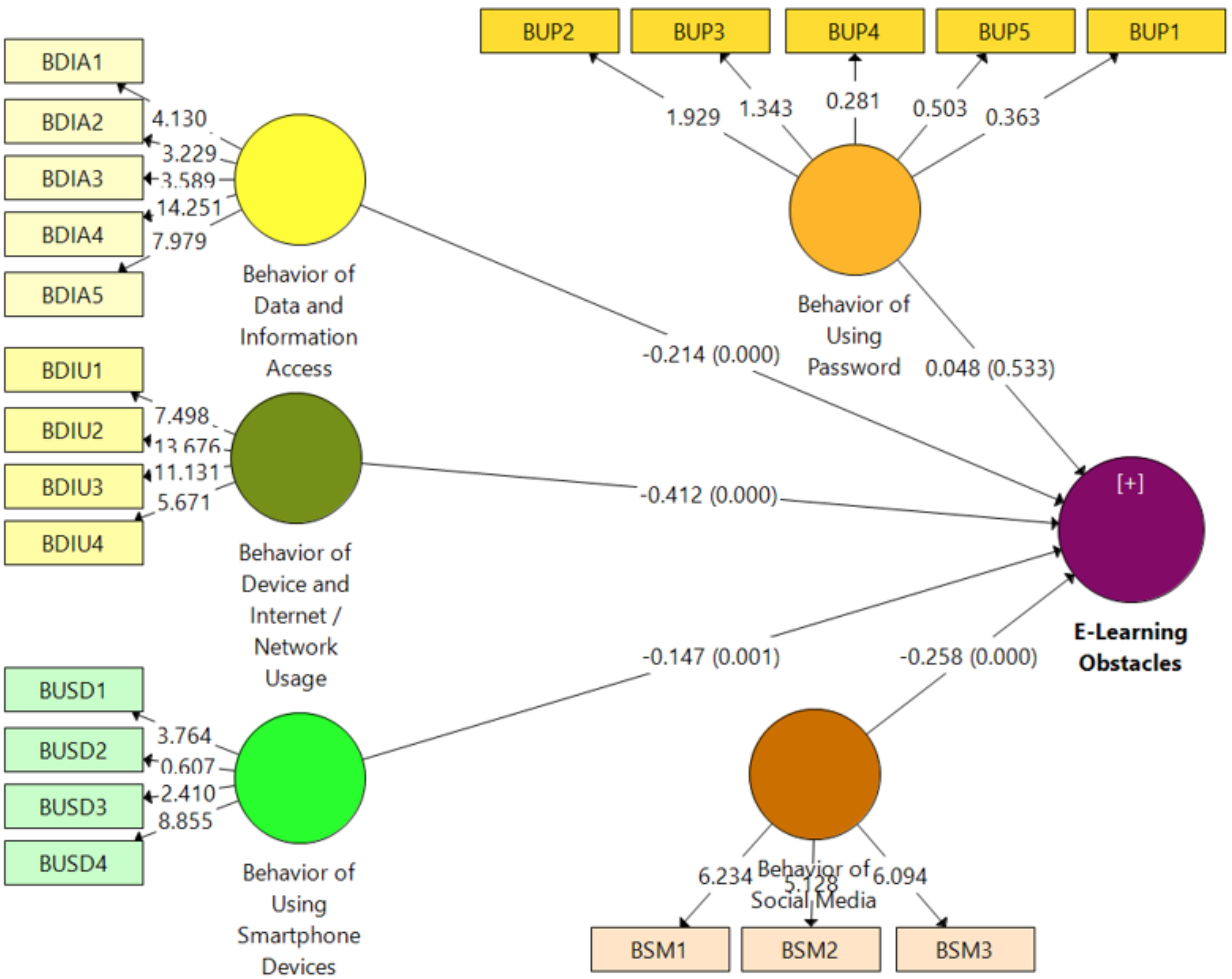

Figure 4: Effect of Cybersecurity Vulnerability Dimensions on E-Learning Obstacles

Table 6: Results of Hypothesis Testing

Path	B	t-value	P-value	95% Bias-Corrected CI		Remark
				LB	UB	
H1: *Cybersecurity Vulnerability Behavior -> E-Learning Obstacles*	-0.555	11.943	<.001	-0.632	-0.453	Supported
H1.1: *Behavior of Data and Information Access -> E-Learning Obstacles*	-0.214	4.506	<.001	-0.294	-0.118	Supported
H1.2: *Behavior of Device and Internet / Network Usage -> E-Learning Obstacles*	-0.412	8.648	<.001	-0.506	-0.32	Supported
H1.3: *Behavior of Social Media -> E-Learning Obstacles*	-0.258	6.396	<.001	-0.337	-0.18	Supported
H1.4: *Behavior of Using Password -> E-Learning Obstacles*	0.048	0.623	0.533	-0.073	0.232	Not Supported
H1.5: *Behavior of Using Smartphone Devices -> E-Learning Obstacles*	-0.147	3.476	0.001	-0.224	-0.058	Supported
H1.6: *Cybersecurity Vulnerability Behavior -> Electronic and physical obstacles*	-0.421	9.128	<.001	-0.492	-0.312	Supported
H1.7: *Cybersecurity Vulnerability Behavior -> Financial and organizational obstacleS*	-0.395	8.658	<.001	-0.461	-0.279	Supported
H1.8: *Cybersecurity Vulnerability Behavior -> Professional and human obstacles*	-0.581	20.03	<.001	-0.622	-0.518	Supported

CI=Confidence Interval; LB=Lower Bound; UB=Upper Bound.

Furthermore, in Table 5 and Figure 5, the Cybersecurity Vulnerability Behavior construct yielded a significant negative effect on E-Learning Obstacles dimensions as follows: Electronic and physical obstacles (β=-0.421,P<0.001), Financial and organizational obstacles (β=-0.395,P<0.001), and Professional and human obstacles (β=-0.581,P<0.001).

The results in Table 7 indicate that about 31% of the variation in E-Learning Obstacles is explained by the variation in Cybersecurity Vulnerability Behavior with a high Cohen's effect size (f2 =0.444). The effect sizes of the other hypotheses were reported and ordered in Figure 6. Then, the predictive relevance was determined by assessing the Stone-Geisser's Q2 Blindfolding, a sample reuse technique that can be used to calculate Q2 values for latent variables. The blindfolding procedure was followed and the Q2 values were calculated for the E-Learning Obstacles (Q2 =0.049). All the values were higher than zero, thus indicating a predictive relevance for endogenous latent variables in the current study' PLS path model (Leguina, 2015; Wetzels et al., 2009). The Goodness of Fit (GoF) was introduced by (Tenenhaus et al., 2005) as a global fit metric (Wetzels et al., 2009).

The GoF criterion for determining if GoF values are too little, too moderate, or too high to be considered a globally adequate PLS model. The GOF value (0.314) was greater than 0.25, indicating moderate fit, so it can be safely concluded that the GoF model is good enough to be considered a sufficiently valid global PLS model. All hypotheses were verified and the outcomes confirm that there is an effective relationship between cybersecurity vulnerability behavior and e-learning obstacles. Also, there are influencing relationships and varying proportions among the dimensions for each of the two variables. Figure (6) explains them in detail that are arranged according to their importance. All hypotheses were fulfilled in varying proportions, even if they were few, except for the sub-hypothesis 1.4, whose percentage was very low and was not supported.

7 Discussion

The current study outcomes confirmed that the professional and human obstacles have a high association with cybersecurity vulnerability behavior. This might be due to the students' poor experience in using modern technologies, and most students have no proficiency in English language and remain unfamiliar with the scientific terminology. Further, the conventional training programs too add fuel to the fire. In most of the cyberattacks, the victims are

either duped by a malicious portrayal or it occurs as a result of lack of cybersecurity knowledge. This finding alarms the educational institutions to develop a sense of belonging and awareness among the students about cybersecurity issues because it not only affects the students' themselves, but also the entire e-learning portal users, technical infrastructure developed by the university/educational institution and so on. With increasing instances of human rights violations on the internet and telecommunication modes, it is important to develop and nurture a healthy ecosystem for the online learning education system, which is possible only through the establishment of a strong, vibrant and secure cyber-communication environment (AbdulAmeer et al., 2022).

The study also found that the overall obstacles have a significant effect on the cybersecurity vulnerability behavior. This finding is in line with the literature pertaining to Iraqi and other MENA countries' educational institutions since in the aftermath of COVID-19, most educational institutions started preferring hybrid mode of education due to health advisories, increasing cost of infrastructure and so on. (Hameed, 2023) listed various obstacles towards the widespread adoption of e-learning in Iraq in terms of educational institutions, student learners, faculty members and so on. According to the authors, students feel isolated and becomes introvert through e-learning mode of education while they lack sufficient socialization skills, lack face-to-face interaction with faculty members and are afraid of facing the real-world scenarios. Cyberattacks pose a significant risk while the students also face difficulties in meeting the technical infrastructure requirements.

The study findings emphasized the importance of using advanced devices, high-speed internet connectivity, access to uninterrupted power and the absence of cyberattacks. Because, these factors tend to affect the mindset of the students. It is important for the student to gain motivation for attention, to gain confidence on the learning outcomes, satisfied over the learning objectives and stay relevant to the job market (Yahiaoui et al., 2022). The current study findings confirm that using smart devices may come as an obstacle towards e-learning while the social media behavior also have an impact on digital learning outcomes. On the contrary, the quantitative study conducted among 185 Iraqi students and lecturers (Al-Malah et al., 2021), the

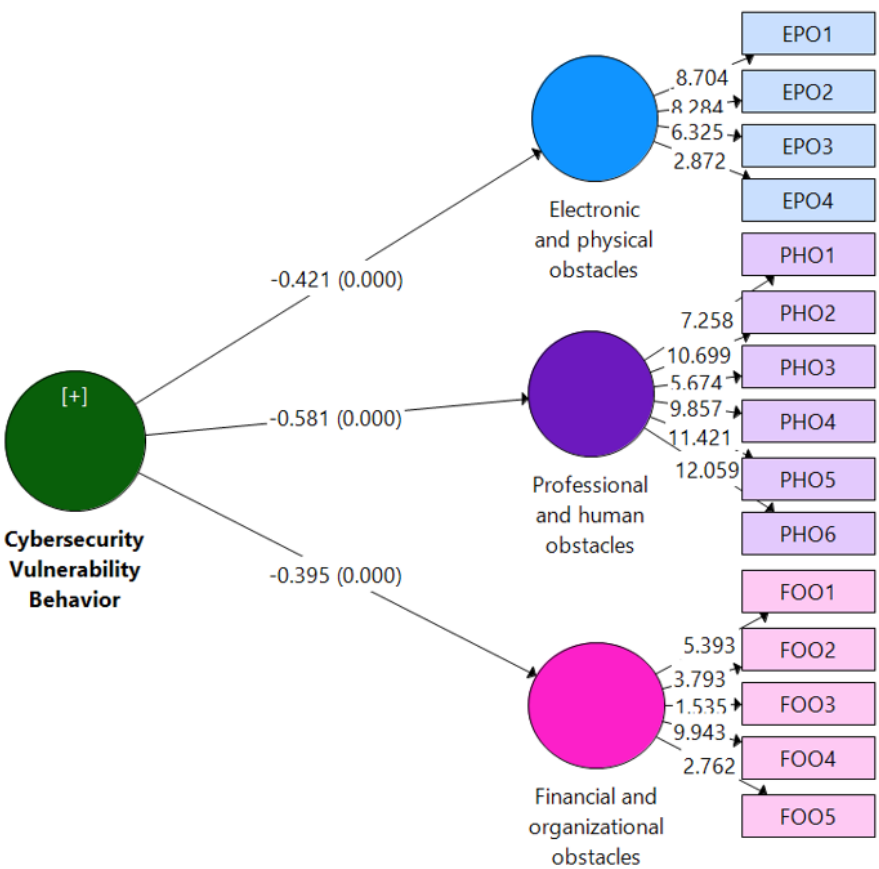

Figure 5: Effect of Cybersecurity Vulnerability Behavior on E-Learning Obstacles Dimensions

Table 7: Structural model assessment

Path	R-Square	R-Square Adjusted	Q Square	F-Square	VIF
Cut-off	***> 0.1***		***> 0***	***> 0.02***	***<5***
Cybersecurity Vulnerability Behavior -> E-Learning Obstacles	0.308	0.306	0.049	0.444	1
Behavior of Data and Information Access -> E-Learning Obstacles	0.445	0.437	0.067	0.072	1.153
Behavior of Device and Internet / Network Usage -> E-Learning Obstacles				0.238	1.286
Behavior of Social Media -> E-Learning Obstacles				0.114	1.051
Behavior of Using Password -> E-Learning Obstacles				0.004	1.046
Behavior of Using Smartphone Devices -> E-Learning Obstacles				0.036	1.089
Cybersecurity Vulnerability Behavior -> Electronic and physical obstacles	0.177	0.175	0.053	0.215	1
Cybersecurity Vulnerability Behavior -> Financial and organizational obstacles	0.156	0.154	0.028	0.185	1
Cybersecurity Vulnerability Behavior -> Professional and human obstacles	0.337	0.335	0.102	0.509	1

Cut-off values reference: (Leguina, 2015; Wetzels et al., 2009)

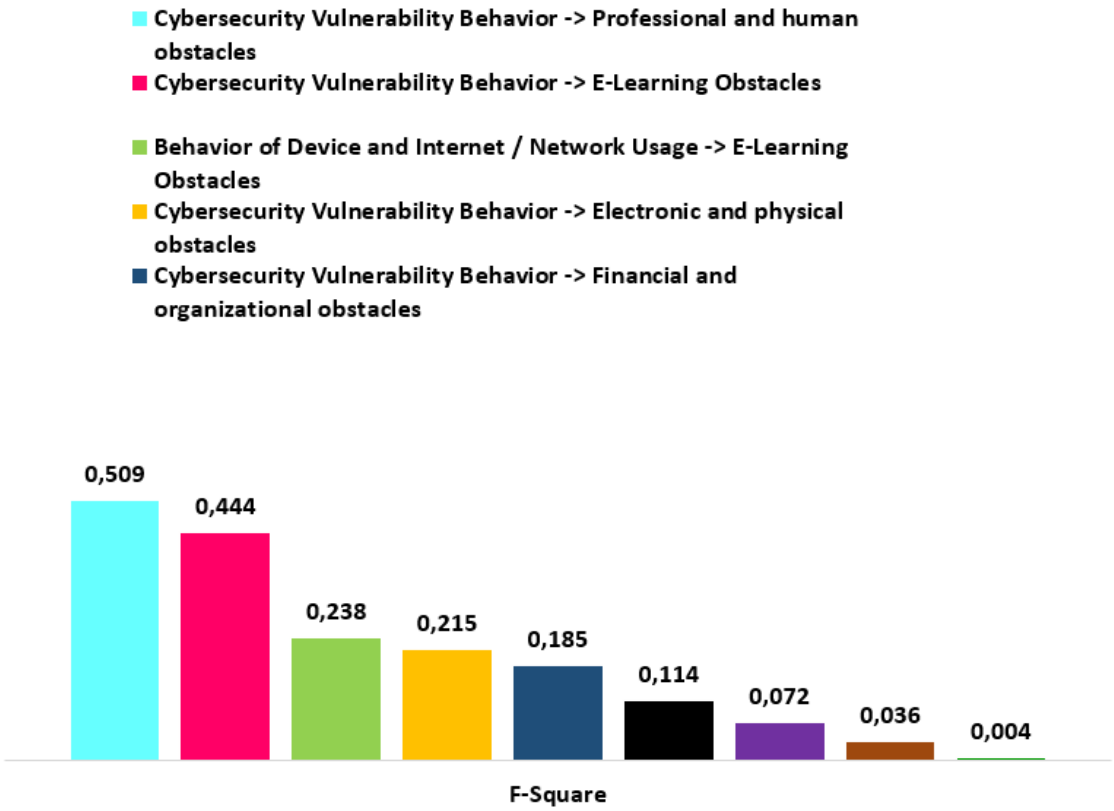

Figure 6: Effect sizes arranged in the order of highest to the lowest

authors found that the digital educational activities, when they are provided in the form of social media, can increase the attentiveness among the students and also attracts them towards the education. It also increases the self-learning motivation. Though the findings may contradict, given the circumstances, environment where the study was conducted, sample population and the possible bias, it can be considered as a suggestion for the future researchers to further explore in this domain.

(Mohamed & Kim, 2023) recommended that the educational institutions must devise their strategies to align with remote learning in a comprehensive and a holistic manner. As per the current study findings, all the hypotheses have been supported (except one) based on which the authors recommend the educational institutions and the governments to focus on developing the technical infrastructure, update the curricula as per the international standards, original applications for the computers, high-speed internet connectivity, conduct awareness programs among the students about cybersecurity issues and the ways to overcome the challenges, refresher training workshops for the faculty members and develop strategies to meet the digital learning requirements in line with the international standards.

8 Conclusion

The current study is a first-of-its-kind attempt to determine the relationship between cybersecurity vulnerability behavior and the obstacles present in e-learning while the study found that the professional and human obstacles had a heavy impact on the cybersecurity vulnerability behaviour. The findings help the educational institutions, policy makers in the governments, cybersecurity experts in the country, students, their parents, faculty members and all the stakeholders involved in imparting digital mode of education to the students in higher educational institutions. There is an urgent need for deploying highly qualified technical staff who are specialized in English language as well as computer proficient. Advanced human-oriented and social engineering strategies must be framed by the educational institutions to overcome the obstacles of e-learning. Future researchers must explore the challenges faced by other university students in Iraq so that a collective initiative can be taken by the educational institutions to bring a digital reform in the country.

Literature

Abbas, A. A. (2020). Educational Competition as a Moderating variable of the relationship between electronic management and intelligent organizations. *Revista Tempos e Espaços Em Educação*, *13*(32), 25. https://doi.org/10.20952/revtee.v13i32.13173

Abdelfattah, F., Al Alawi, A. M., Dahleez, K. A., & El Saleh, A. (2023). Reviewing the critical challenges that influence the adoption of the e-learning system in higher educational institutions in the era of the COVID-19 pandemic. *Online Information Review*, *47*(7), 1225–1247. https://doi.org/10.1108/OIR-02-2022-0085

AbdulAmeer, S. A., Saleh, W. R., Hussam, R., Al-Hareeri, H., Alghazali, T., S. Mezaal, Y., & Saeed, I. N. (2022). Cyber Security Readiness in Iraq: Role of the Human Rights Activists. *International Journal of Cyber Criminology*, *16*(2), 1–14

Abdulhassan Abbas, A., & Hurajah Al Hasnawia, H. (2020). Role of Psychological Contract Breach and Violation in Generating Emotional Exhaustion: The Mediating Role of Job Procrastination. *Cuadernos de Gestión*. https://doi.org/ https://doi.org/10.5295/cdg.181021aa

Abdulla, R., Faraj, H., Abdullah, C., Amin, A., & Rashid, T. (2023). Analysis of Social Engineering Awareness Among Students and Lecturers. *IEEE Access*, *PP*, 1. https://doi.org/10.1109/ACCESS.2023.3311708

Abed, M. G., Abdulbaqi, R. F., & Shackelford, T. K. (2022). Saudi Arabian Students' Beliefs about and Barriers to Online Education during the COVID-19 Pandemic. *Children (Basel, Switzerland)*, *9*(8). https://doi.org/10.3390/children9081170

Abeer, Q. (2022). Obstacles To Effective Use Of E-Learning In Higher Education From The Viewpoint Of Faculty Members. *Turkish Online Journal of Distance Education-TOJDE*, *23*(1), 144–177. https://files.eric.ed.gov/fulltext/EJ1329784.pdf

Aborujilah, H. A., Al-Alawi, E., Al-Hidabi, D., & Al-Othmani, A. (2022). *Exploring Critical Challenges and Factors Influencing E-Learning Systems Security During COVID-19 Pandemic*. https://doi.org/10.1109/ITSS-IoE56359.2022.9990935

Abumandour, E.-S. T. (2022). Applying e-learning system for engineering education–challenges and obstacles. *Journal of Research in Innovative Teaching & Learning*, *15*(2), 150–169.

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(01), 1650007. https://doi.org/10.1142/S0219649216500076

Al-kaaf, H. A. (2023). *Machine Learning Approaches for Kids' E-learning Monitoring BT - Kids Cybersecurity Using Computational Intelligence Techniques* (W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, & A. Emara (eds.); pp. 25–36). Springer International Publishing. https://doi.org/10.1007/978-3-031-21199-7_2

Al-Malah, D., Abbas, A., Majeed, B., & Alrikabi, H. (2021). The Influence E-Learning Platforms of Undergraduate Education in Iraq. *International Journal*

of Recent Contributions from Engineering Science & IT (IJES), *9*, 90–99. https://doi.org/10.3991/ijes.v9i4.26995

Al-Sherideh, A. S., Maabreh, K., Maabreh, M., Mousa, M. R. Al, & Asassfeh, M. (2023). Assessing the Impact and Effectiveness of Cybersecurity Measures in e-Learning on Students and Educators: A Case Study. *International Journal of Advanced Computer Science and Applications*, *14*(5). https://doi.org/10.14569/IJACSA.2023.0140516

Al-Tae, A. K. J., Al-Dhalimi, H. A.-H., & Al- Shaibani, A. K. (2022). Relationship of Cybersecurity and the National Securityofthe Country: Iraq Case Study. *Sys Rev Pharm*, *11*(12), 469–476. https://www.sysrevpharm.org/articles/relationship-of-cybersecurity-and-the-national-security-of-the-country-iraq-case-study.pdf

Al Shabibi, A. M., & Al-Suqri, M. N. (2023). *Cybersecurity Awareness Among Students During the COVID-19 Digital Transformation of Education: A Case Study at the Muscat (Oman) Schools BT - Future Trends in Education Post COVID-19* (H. M. K. Al Naimiy, M. Bettayeb, H. M. Elmehdi, & I. Shehadi (eds.); pp. 39–51). Springer Nature Singapore.

Al Shamari, D. (2022). Challenges and barriers to e-learning experienced by trainers and training coordinators in the Ministry of Health in Saudi Arabia during the COVID-19 crisis. *PloS One*, *17*(10), e0274816. https://doi.org/10.1371/journal.pone.0274816

Alhamdawee, N. (2023). *online learning in Iraq challanges and opportunities*. *4*, 1...7.

Almaiah, M. A., Al-Khasawneh, A., & Althunibat, A. (2020). Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies*, *25*(6), 5261–5280. https://doi.org/10.1007/s10639-020-10219-y

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

Ameen, N., Willis, R., & Abdullah, M. (2017). *The use of e-learning by students in Iraqi universities:Potential and challenges*. https://doi.org/10.23918/vesal2017.a27

Arul, E., & Punidha, A. (2022). Artificial Intelligence to Protect Cyber Security Attack on Cloud E-Learning Tools (AIPCE). *International Conference on Computing, Communication, Electrical and Biomedical Systems*, 29–37.

Barakat, M., Farha, R. A., Muflih, S., Al-Tammemi, 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), e09928. https://doi.org/https://doi.org/10.1016/j.heliyon.2022.e09928

Bottyan, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences*, *13*(3 SE-Articles and Studies), ArtNo: 363. https://doi.org/10.24368/jates363

Byrne, B. (2016). *Structural equation modeling with AMOS*. Routledge.

Darawsheh, S. R., Alshurideh, M., Al-Shaar, A. S., Barsom, R. M. M., Elsayed, A. M., & Ghanem, R. A. A. A. (2023). *Obstacles to Applying the E-Learning Management System (Blackboard) Among Saudi University Students (In the College of Applied Sciences and the College of Sciences and Human Studies) BT - The Effect of Information Technology on Business and Marketing Intelligence Systems* (M. Alshurideh, B. H. Al Kurdi, R. Masa'deh, H. M. Alzoubi, & S. Salloum (eds.); pp. 389–414). Springer International Publishing. https://doi.org/10.1007/978-3-031-12382-5_21

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *J Med Internet Res*, *26*, e46904. https://doi.org/10.2196/46904

Faez Hasan, M., & Al-Ramadan, N. S. (2021). Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. *Social Science and Humanities Journal*, *5*(8), 2312–2323.

Fauzi, M. A. (2022). E-learning in higher education institutions during COVID-19 pandemic: current and future trends through bibliometric analysis. *Heliyon*, *8*(5), e09433. https://doi.org/https://doi.org/10.1016/j.heliyon.2022.e09433

Geogiana Buja, A., Deraman, N. A., Wahid, S. D. M., & Mohd Isa, M. A. (2021). Cyber Security Featuresfor National E-Learning Policy. *Turkish Journal of Computer and Mathematics Education*, *12*(5), 1729–1735. https://turcomat.org/index.php/turkbilmat/article/download/2169/1889/4085

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, *105*, 410–431. https://doi.org/https://doi.org/10.1016/j.future.2019.12.018

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate Data Analysis* (7th ed.). Pearson.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks.

Hameed, L. M. (2023). E-learning in Iraq from Defensive to supportive Strategies: Facts and Obstacles. *Proceedings of the Iraqi Academics Syndicate 3rd International Conference on Arts and Humanities Sciences*.

Ibrahim, A. F., Attia, A. S., Bataineh, A. M., & Ali, H. H. (2021). Evaluation of the online teaching of architectural design and basic design courses case study: College of Architecture at JUST, Jordan. *Ain Shams En-*

gineering Journal, *12*(2), 2345–2353. https://doi.org/https://doi.org/10.1016/j.asej.2020.10.006

Ibrahim, A. H., Madhush, qadir eabd alhusayn, & Farhan, B. I. (2019). Obstacles to the application of e - learning in the Faculty of Information University of Dhi Qar. *Lark Journal for Philosophy, Linguistics and Social Sciences*, *2*(33), 306–315.

K. Elberkawi, E., Maatuk, A., F. Elharish, S., & M. Eltajoury, W. (2022). A Comparative Study of the Challenges and Obstacles Facing E-Learning During the COVID-19 Pandemic from the Perspectives of University Instructors and Students. *Proceedings of the 2022 Australasian Computer Science Week*, 186–192. https://doi.org/10.1145/3511616.3513114

Khadija Hassan, S., & Mustafa Jawad, R. (2022). Internal and External Factors to Adopt a Cyber Security Strategy in Iraqi Organisations. *Webology*, *19*(1), 5181–5198. https://www.webology.org/data-cms/articles/20220123025726pmWEB19349.pdf

Khan, M., Nabi, M. K., Khojah, M., & Tahir, M. (2020). Students' perception towards e-learning during COVID-19 pandemic in India: An empirical study. *Sustainability*, *13*(1), 57.

Khan, N. F., Ikram, N., Saleem, S., & Zafar, S. (2022). Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. In *Security Journal* (pp. 1–33). https://doi.org/10.1057/s41284-022-00343-4

Khan, N. T., & Ahmed, S. (2018). Impact of Facebook addiction on studentsacademic performance. *Research Medical and Engineering Sciences*, *5*(2), 424–426.

Khlifi, Y. (2020). An Advanced Authentication Scheme for E-evaluation Using Students Behaviors Over E-learning Platform. *International Journal of Emerging Technologies in Learning (IJET)*, *15*(04 SE-Papers), 90–111. https://doi.org/10.3991/ijet.v15i04.11571

Klaib, A. A., Talooh, M. A. M., & Arbi, A. (2022). E-Learning, Challenges and Opportunities of Instructors in Libyan Higher Institutes. *International Conference on Engineering & MIS (ICEMIS)*, 1–6.

Kumar, A., Pandit, A., & Singh, S. (2022). Reliable Cyber Security And Improvement In E-Learning System. *Journal of Positive School Psychology*, *6*(11), 1743–1752. https://journalppw.com/index.php/jpsp/article/view/14307/9274

Leguina, A. (2015). A primer on partial least squares structural equation modeling (PLS-SEM). *International Journal of Research & Method in Education*, *38*(2), 220–221. https://doi.org/10.1080/1743727X.2015.1005806

Maatuk, A. M., Elberkawi, E. K., Aljawarneh, S., Rashaideh, H., & Alharbi, H. (2022). The COVID-19 pandemic and E-learning: challenges and opportunities from the perspective of students and instructors. *Journal of Computing in Higher Education*, *34*(1), 21–38.

MacKenzie, S. B., & Podsakoff, P. M. (2012). Common Method Bias in Marketing: Causes, Mechanisms, and Procedural Remedies. *Journal of Retailing*, *88*(4), 542–555. https://doi.org/https://doi.org/10.1016/j.jretai.2012.08.001

Mohamed, O., & Kim, J. (2023). Adult E-Learning Issues in Middle East Educational Organizations Due to Covid-19 Pandemic: Challenges and Recommendations. *Https://Newprairiepress.Org/Aerc*. https://newprairiepress.org/cgi/viewcontent.cgi?article=4318&context=aerc

Mojarad, F. A., Hesamzadeh, A., & Yaghoubi, T. (2023). Exploring challenges and facilitators to E-learning based Education of nursing students during Covid-19 pandemic: a qualitative study. *BMC Nursing*, *22*(1), 278. https://doi.org/10.1186/s12912-023-01430-6

Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. *Computers in Human Behavior*, *158*, 108274. https://doi.org/https://doi.org/10.1016/j.chb.2024.108274

Muhammad, F. J. (2022). E-learning and The Obstacles to its Application From The Point of View of Secondary School Teachers. *Basic Education College Magazine For Educational and Humanities Sciences*, *14*(57).

Nagham Oudeh Alhamdawee. (2023). Online Learning In Iraq: Challenges And Opportunities. *European Journal of Humanities and Educational Advancements*, *4*(1 SE-), 1–7. https://scholarzest.com/index.php/ejhea/article/view/3089

Pandian, T. (2023). Information And Multimedia Security In An Online Learning Environment. *INTED2023 Proceedings*, 1166–1171.

Peng, B. (2023). Analysis on the Relationships of Smartphone Addiction, Learning Engagement, Depression, and Anxiety: Evidence from China. *Iranian Journal of Public Health*, *52*(11), 2333–2342. https://doi.org/10.18502/ijph.v52i11.14033

Salman, A. M., & Shahadab, F. H. (2022). Obstacles of Teaching Distance Universities Courses in Light of E-Learning Quality Standards. *Cypriot Journal of Educational Sciences*, *17*(4), 1244–1257.

Sefriani, R., Yunus, Y., Ambiyar, Syah, N., & Fadhilah. (2023). Correlation of Social Media Addiction to Academic Achievement in E-Learning. *Indonesian Journal of Computer Science*, *12*. https://doi.org/10.33022/ijcs.v12i6.3581

Sobaih, A. E. E., Palla, I. A., & Baquee, A. (2022). Social Media Use in E-Learning amid COVID 19 Pandemic: Indian Students' Perspective. *International Journal of Environmental Research and Public Health*, *19*(9). https://doi.org/10.3390/ijerph19095380

Sunday, O. J., Adesope, O. O., & Maarhuis, P. L. (2021). The effects of smartphone addiction on learning: A me-

ta-analysis. *Computers in Human Behavior Reports*, *4*, 100114. https://doi.org/https://doi.org/10.1016/j.chbr.2021.100114

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. *Information & Management*, *57*(6), 103334. https://doi.org/https://doi.org/10.1016/j.im.2020.103334

Tarrad, K. M., Al-Hareeri, H., Alghazali, T., Ahmed, M., Al-Maeeni, M. K. A., Kalaf, G. A., E. Alsaddon, R., & S. Mezaal, Y. (2022). Cybercrime Challenges in Iraqi Academia: Creating Digital Awareness for Preventing Cybercrimes. *International Journal of Cyber Criminology*, *16*(2), 15–31.

Tenenhaus, M., Vinzi, V. E., Chatelin, Y.-M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis*, *48*(1), 159–205. https://doi.org/https://doi.org/10.1016/j.csda.2004.03.005

Vishal Verma, & Janardan Pawar. (2024). Assessment Of Students Cybersecurity Awareness And Strategies To Safeguard Against Cyber Threats. *Journal of Advanced Zoology*, *45*(S4 SE-Articles), 82–89. https://doi.org/10.53555/jaz.v45iS4.4156

Wetzels, M., Odekerken-Schroder, G., & van Oppen, C. (2009). Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. *MIS Quarterly*, *33*(1), 177–195. https://aisel.aisnet.org/misq/vol33/iss1/11/

Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(3), 395–399. https://doi.org/10.32736/sisfokom.v9i3.1021

Yahiaoui, F., Aichouche, R., Chergui, K., Brika, S. K. M., Almezher, M., Musa, A. A., & Lamari, I. A. (2022). The Impact of e-Learning Systems on Motivating Students and Enhancing Their Outcomes During COVID-19: A Mixed-Method Approach. *Frontiers in Psychology*, *13*. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.874181

Yeh, C.-Y., & Tsai, C.-C. (2022). Massive Distance Education: Barriers and Challenges in Shifting to a Complete Online Learning Environment. *Frontiers in Psychology*, *13*. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.928717

Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework. *Journal of Applied Security Research*, *18*(2), 267–288. https://doi.org/10.1080/19361610.2021.1989271

Zahid, I., Hussein, S., & Mahdi, S. (2023). Measuring Individuals Cybersecurity Awareness Based on Demographic Features. *Iraqi Journal for Electrical and Electronic Engineering*, *20*, 58–67. https://doi.org/10.37917/ijeee.20.1.6

Zhang, C., Hao, J., Liu, Y., Cui, J., & Yu, H. (2022). Associations Between Online Learning, Smartphone Addiction Problems, and Psychological Symptoms in Chinese College Students After the COVID-19 Pandemic. *Frontiers in Public Health*, *10*, 881074. https://doi.org/10.3389/fpubh.2022.881074

Zhang, J., & Zeng, Y. (2024). Effect of College Students' Smartphone Addiction on Academic Achievement: The Mediating Role of Academic Anxiety and Moderating Role of Sense of Academic Control. *Psychology Research and Behavior Management*, *17*, 933–944. https://doi.org/10.2147/PRBM.S442924

Zou, C., Li, P., & Jin, L. (2022). Integrating smartphones in EFL classrooms: students' satisfaction and perceived learning performance. *Education and Information Technologies*, *27*(9), 12667–12688. https://doi.org/10.1007/s10639-022-11103-7

Ibrahim Mohamed Taha: I hold a master's degree in statistics. I have experience working on many advanced statistical programs. I currently work at Sadat University. I have a number of research papers published in Arab journals.

Rajaa Hussein Abd Ali: I hold a Master's and PhD from the University of Babylon/College of Science/ Department of Physics. I have experience in the field of English editing. I have experience in the field of statistical programs.

Ali Abdulhassan Abbas: I have a master's degreefrom the University of Karbala College of Administrationand Economics in the field of Production Managementand Operations in the year 2005. I have also obtained aPh.D. from Karbala University, College of Administrationand Economics in Organizational Behavior and HumanResources Management in 2014. I currently work atKarbala University, College of Administration andEconomics in the Accounting Department. I havetaught many subjects in my specific area, as well as inother areas. I have also taught Financial Managementfor postgraduate studies. I have translated 4 books onbusiness administration into Arabic. I have numerousresearch papers published in local and internationaljournals.

Vpliv vedenja študentov glede ranljivosti kibernetske varnosti na ovire pri e-učenju

Povzetek Ozadje/Namen: Študija preučuje razmerje med vedenjem študentov glede ranljivosti kibernetske varnosti in ovirami pri e-učenju. Z hitrim razvojem spletnega izobraževanja je zagotavljanje varnosti in zasebnosti digitalnih platform postalo ključno. V tem kontekstu je trenutna študija prvi poskus razumevanja razmerja med tema dvema spremenljivkama v ozadju visokošolskih ustanov v Iraku.
Metode: Za to študijo so raziskovalci leta 2023 zbrali podatke od študentov, starih med 19 in 25 let, vpisanih na Univerzo v Karbali, Irak, z uporabo polstrukturiranega raziskovalnega vprašalnika, izbranih z metodo naključnega vzorčenja. Vprašalnik je vseboval vprašanja, povezana z dimenzijami tako odvisne kot neodvisne spremenljivke. Skupno je bilo za analizo upoštevanih 350 veljavnih odgovorov, pri čemer je bila izvedena metoda PLS-SEM.
Rezultati: Rezultati so pokazali, da imajo strokovne in človeške ovire visoko povezavo z vedenjem glede ranljivosti kibernetske varnosti. Študija je tudi ugotovila, da imajo splošne ovire pomemben vpliv na vedenje glede ranljivosti kibernetske varnosti. Vse hipoteze so bile preverjene in rezultati potrjujejo, da obstaja učinkovito razmerje med vedenjem glede ranljivosti kibernetske varnosti in ovirami pri e-učenju.
Zaključek: Na podlagi rezultatov študije so avtorji predlagali nekaj priporočil za vse deležnike v procesu e-učenja, kot so izobraževalne ustanove, vlade, člani fakultete, študenti in njihovi starši. Čeprav je bila trenutna študija omejena na eno univerzo v Iraku, se lahko prihodnji raziskovalci osredotočijo na razširitev študije na druge visokošolske ustanove, da bi na podlagi raziskovalnih dokazov lahko pripravili nacionalno pobudo na ravni politike.

Ključne besede: *Vedenje glede ranljivosti kibernetske varnosti, Ovire pri e-učenju, Visokošolsko izobraževanje, PLS-SEM, Motivacija študentov, Vedenje pri učenju*