2023

Towards sustainable e-learning platforms in the context of cybersecurity: A TAM-driven approach

Hebah Alquran

Towards Sustainable E-Learning Platforms in the Context of Cybersecurity: A TAM-Driven Approach

by

Hebah Alquran

Dissertation

Submitted to the GameAbove College of Engineering and Technology

Eastern Michigan University

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

Technology

Concentration in Cybersecurity and Information Assurance

Dissertation Committee:

Bilquis Ferdousi, PhD, Committee Chair

Munther Abualkibash, PhD

Robert Carpenter, PhD

Dorothy McAllen, PhD

June 13, 2023

Ypsilanti, Michigan

Acknowledgments

I would like to express my heartfelt gratitude and special thanks to my parents, husband, family, advisor, and the committee members, those who have supported me throughout the journey of writing this dissertation. First and foremost, I would like to thank my parents, dad and mom, Khaled and Fatimah for their unwavering love and support. Their encouragement and belief in me have been a source of strength, motivation and success.

My dear husband Shadi, who has always been my rock, has provided me with unwavering support and encouragement. His love and understanding have been invaluable to me. His patience, care and encouragement made it possible for me to balance my responsibilities as a wife, mother and a student. My piece of heart, my children Sarah and Mohammad, who have brought joy and laughter into my life, have always been a source of inspiration to me. Their hugs and smiles were the light of my life during the most challenging times. They have taught me the importance of persistence, determination, and perseverance. For My sisters and brothers, thank you for being there for me, and for being the best siblings anyone could ask for.

I am deeply grateful to my family in law, especially my father-in-law, Elaiyan for their pride, support, and encouragement throughout my academic journey. Their unwavering belief in me has been a constant source of inspiration and motivation. I would also like to acknowledge the love and acceptance they have shown me since joining their family, which has made this journey all the more meaningful.

I would also like to extend my sincere gratitude to my advisor, Dr. Bilquis Ferdousi, for her guidance, support, and encouragement throughout my academic journey. Her wisdom, insights, and expertise have been invaluable in accomplishing this dissertation. Her expertise, enthusiasm and encouragement have been instrumental in shaping my academic and professional goals.

I would like to thank the profound members of my committee, Dr. Dorothy McAllen, Dr. Robert Carpenter, and Dr. Munther Abulkibash, for their valuable time, effort, and feedback. Their constructive comments and suggestions have been instrumental in improving the quality of this dissertation. I am deeply appreciative of the time and energy they have generously given to reviewing my work and provide me with constructive criticism, which has helped me to refine my ideas and improve my writing.

I would also like to extend my gratitude to Eastern Michigan University (EMU) that provided financial support for my journey in the PhD program as well as gave me a fruitful teaching experience as an adjunct in its school (Information Security and Applied Computing). Finally, I would like to acknowledge all the individuals who have supported me throughout my academic journey, including friends, colleagues, and classmates. Your encouragement and support have been truly invaluable.

This dissertation would not have been possible without the support of all of you, and I am truly grateful to each and every one of you for your support and encouragement. Your contribution to this journey was immeasurable. I hope that this achievement will bring a smile to all of your faces, and that you will all share in my joy. Thank you from the bottom of my heart!

Abstract

The rapid growth of electronic learning (e-learning) platforms has raised concerns about cybersecurity risks. The vulnerability of university students to cyberattacks and privacy concerns within e-learning platforms presents a pressing issue. Students' frequent and intense internet presence, coupled with their extensive computer usage, puts them at higher risk of being a potential victim of cyberattacks. This problem necessitates a deeper understanding in order to enhance cybersecurity measures and safeguard students' privacy and intellectual property in educational environments. This dissertation work addresses the following research questions: (a) To what extent do *cybersecurity perspectives* affect student's intention to use e-learning platforms? (b) To what extent do students' *privacy concerns* affect their intention to use e-learning platforms? (c) To what extent does students' *cybersecurity awareness* affect their intention to use e-learning platforms? (d) To what extent do *academic integrity concern***s** affect their intention to use e-learning platforms? and (e) To what extent does students' *computer self-efficacy* affect their intention to use e-learning platforms? This study was conducted using an enhanced version of the technology acceptance model (TAM3) to examine the factors influencing students' intention to use e-learning platforms. The study involved undergraduate and graduate students at Eastern Michigan University, and data were collected through a web-based questionnaire. The questionnaire was developed using the Qualtrics tool and included validated measures and scales with close-ended questions. The collected data were analyzed using SPSS 28, and the significance level for hypothesis testing was set at 0.05. Out of 6,800 distributed surveys, 590 responses were received, and after data cleaning, 582 responses were included in the final sample. The findings revealed that cybersecurity perspectives, cybersecurity awareness, academic integrity concerns, and computer self-efficacy significantly influenced students’ intention to use e-learning platforms. The study has implications for practitioners, educators, and researchers involved in designing secure e-learning platforms, emphasizing the importance of cybersecurity and recommending effective cybersecurity training programs to enhance user engagement. Overall, the study highlights the role of cybersecurity in promoting the adoption and usage of e-learning platforms, providing valuable insights for developers and educators to create secure e-learning environments and benefiting stakeholders in the e-learning industry.

Table of Content

List of Tables

List of Figures

Chapter One: Introduction

Problem Statement

The development of information and communication technology and the increased interest in the use of this advanced technology have built a new virtual academic world in higher learning through which instructors, students, and academic administrators are conducting their educational process. The electronic learning (e-learning) environment is the space where students need to trust learning management systems (LMSs) and where procedures are expected to ensure a complete protection of students' information, discussions, grades (Kaiiali et al., 2016), and ideas. An e-learning platform like Canvas has many useful features that were especially helpful during the COVID-19 pandemic (Singh et al., 2021).

Although this digital learning environment is considered useful, since it provides more flexible options to accomplish academic goals, the existence of digital learning has triggered many cyber security risks and concerns that includes data security, privacy, and academic integrity. Therefore, it is crucial to determine the factors that may affect students' decision to accept e-learning platforms considering the above-mentioned factors (Khalaf et al., 2022). This research work sought to provide a better understanding regarding the concerns of threat to cybersecurity and the factors that contribute to it.

In this context, the primary objective of this research was to determine the elements that could influence students' intention to use e-learning platforms. Drawing upon a thorough examination of existing literature, this study put forth five factors as potential predictors. These factors encompass cybersecurity perspectives, privacy concerns, cybersecurity awareness, computer self-efficacy (CSE), and academic integrity (AI) concerns.

Purpose of Study

This research work discusses serious challenges students face when they adopt e-learning platforms. The basic issues studied in this dissertation work are cybersecurity, privacy, and AI concerns as well as the CSE and cybersecurity awareness all of which were incorporated to examine their impact on students' intention to use e-learning platforms after COVID-19. The point of conducting this dissertation was to explore students' intention to use e-learning platforms from cybersecurity perspectives without any forcing conditions based on the five proposed predictors for this study.

There were three main groups of constructs in this framework, the technical cybersecurity-based constructs (i.e., cybersecurity, privacy, and cybersecurity awareness), moral cybersecurity construct (i.e., academic integrity), and psychological construct (i.e., CSE), which represented the intrinsic and non-technical factor. Cybersecurity, awareness, and privacy factors will measure the level of students' trust toward adopting e-learning platforms.

Significance and Relevance

Compared to other demographics, university students exhibit a higher level of internet engagement and computer usage (Jones, 2008). They often enroll in online courses, submit assignments, interact with instructors and fellow students, and even take online exams using internet-based services. Consequently, students are at an increased risk of falling victim to cyberattacks. For this reason, privacy is a serious issue for students. Emails and electronic platforms are used by instructors to communicate sensitive information to students (e.g., names, grades, meeting locations, intellectual property). Furthermore, online proctored exams raise threats to students' privacy because many students feel less comfortable when they take exams since they are being watched and observed. Another reason is that students are concerned regarding the recorded videos after the exams are finished. How will their recording be analyzed or with whom will their sensitive information be shared and for what purposes? All these concerns are triggered as a result of using educational systems connected to the internet networks such as e-learning platforms.

In certain instances, students may lack awareness regarding the duration for which faculty members and other academic service providers retain their information. Additionally, students may not recognize the significance of safeguarding privileged information, such as names, records, account numbers, and other sensitive data, when engaging in online communications with friends or colleagues during school or work-related projects.

A data loss threat is also imminent for students. From one side, the loss or theft of their computers, flash drives, and phones threatens their privacy, confidentiality, and anonymity. A hacking attack or an unauthorized intrusion that results in data loss can further compromise student accounts. Insufficient awareness of cybersecurity threats and the needed knowledge and skills can prevent students from protecting their computers from hackers who can spoof other students' accounts. On the other side, in online classes, students are authenticated and authorized to access their assignments over the e-learning platforms. Assignments such as interactive discussion threads allow students to engage in a discussion by posting their personal ideas and thoughts making them available to other students who can access, read, or share them without the permission of their owner. This illegal or unethical activity threatens the intellectual property of students' content they provide over these platforms. Therefore, it was important to explore students' intention to use e-learning platforms within the cybersecurity context. This dissertation sought to determine the acceptance levels of students towards adopting these platforms according to the five proposed predictors of cybersecurity perspectives, privacy concerns, cybersecurity awareness, CSE, and AI concerns.

In turn, this dissertation can play a significant role in providing a better understanding about the most important concepts and critical risks in digital education and spreading awareness. In order to understand the significant factors related to accepting e-learning platforms by students, it is absolutely necessary to identify what factors contribute to their success. To that end, this dissertation aimed to examine factors rarely tested in e-learning contexts together. An enhanced version of technology acceptance model (TAM3) was the methodological framework to study the impact of cybersecurity perspectives, privacy concerns, cybersecurity awareness, CSE, and AI concerns on students' perceptions regarding their intention to use e-learning platforms. The main objective of this research was to develop an extended TAM3 for the determinants of the intention to use e-learning platforms; in which cybersecurity perspectives, privacy, and cybersecurity awareness represented the perceived usefulness (PU) construct in TAM3, and the CSE and AI concerns represented perceived ease of use (Venkatesh, 2000).

Another reason this dissertation is significant is that previous research has focused on studying e-learning platforms; either psychologically or technically but not together in one study. Technical challenges that students may have struggled with during their remote studying were introduced in the forms of poor internet connection and the inability to afford the cost of internet plans needed to access online classes. Other articles (Azizi et al., 2022; Aldhahi et al., 2022; Meinhardt-Injac and Skowronek, 2022) discussed the psychological and mental impact of COVID-19 on students' perceptions regarding commitment to the online learning environment. Social isolation was a critical concern for many students and their families. Frustration, anxiety, depression, and stress were frequently mentioned issues students suffered from during the pandemic. Unlike those articles, this dissertation work spotlighted both areas from cybersecurity perspectives. Technical, moral, and pedagogical based cybersecurity factors have been proposed and involved as external variables to TAM.

Many articles have been reviewed in this regard. An abundance of research studies has examined the adoption of e-learning platforms from a cybersecurity point of view as well as privacy perceptions which provide definitions and illustration of cybersecurity related aspects. In this dissertation, each of the five proposed factors has been explained elaborately. For example, the most important terms have been defined and clarified in an organized table. Every section in this dissertation was recapped in summarized tables to make it easy for readers who are non-experts in this domain to follow up and understand the main concepts in cybersecurity.

After reviewing more than a hundred articles on cybersecurity in e-learning, it was found that a limited number of studies have utilized technology acceptance model (TAM) or the enhanced versions of TAM (i.e., TAM3) as a framework to examine the adoption of e-learning platforms from cybersecurity perceptions which strengthens and empowers this dissertation work. Especially, in this dissertation, TAM3 has been extended to include the five predictors altogether in one study as external variables.

It is worth mentioning that a part of this dissertation work was accepted for publication in the *International Journal of Scientific Research in Multidisciplinary Studies (IJSRMS)* and was published in November 2022. Finally, this dissertation will assist IT staff to maintain and design a higher quality shell that encompasses the online courses to meet students' needs better and improve student satisfaction (Chang et al., 2022). Finally, the researchers, administrators, and planners in these institutions can benefit from the findings of this study since they present a realistic image of the present e-learning platforms that can be used to improve student use of online education by spot lighting the importance of cybersecurity awareness in dealing with cyber threats in e-learning platforms (Dash & Ansari, 2022).

Dissertation Work Overview

The dissertation provides a logical sequence in writing the structure of this work. For instance, the literature review begins with an overview of the main technology of e-learning. A diagram is included to visualize the access model of e-learning technology. Furthermore, the major properties of security (or cybersecurity requirements), confidentiality, integrity, and availability (CIA), as well as authentication, authorization, and non-repudiation are illustrated in detail in the text in this section as well as summarized in tables. In the next section in the literature review, the most frequent and serious cybersecurity risks in e-learning are categorized into groups to facilitate recognizing every threat's kind and source by providing examples on each. The predictors are explained separately in sub-sections. A summarizing table is included at the end of each predictor's section.

The second part of the literature review consists of theoretical theories as well as the most significant theories that have been adopted in the topic of cybersecurity. The reasoned action theory (TRA) planned behavior theory (PBT), diffusion of innovation theory (DIT), and technology acceptance model (TAM) are the main theories explained in the first part of the background. Then, space transition theory (STT), social identity theory (SIT), protected motivated theory (PMT), compliance theory, and computer ethics theory are discussed in relation to cybersecurity. Two tables summarize recent studies that examined e-learning platforms, showing the type of research design that was conducted (quantitative, qualitative, or mixed), the main constructs, instruments, samples, and findings.

An online questionnaire was used as the instrument to collect data in this study to serve the goals for conducting the dissertation work. Based on the reviewed literature, many questions about cybersecurity perspectives, privacy concerns, cybersecurity awareness, CSE, and AI concerns were aggregated from relevant studies that investigated similar topics. A set of questions were used to rate each construct/scale using a 5-point Likert scale ranging from *strongly disagree* represented by the number 1 and *strongly agree* represented by the number 5 (see Table 1). All of the major variables or constructs in the framework were scaled variables. In contrast, the individual items or questions that belong to each construct were ordinally measured.

Table 1

Constructs' Definition

Term / Concept	Description	Reference
e-Learning Platforms	E-learning is a web-based learning method that utilizes internet-based communication, collaboration, services, knowledge exchange, and training to support learners' active learning regardless of any time limitations or physical barriers.	Lee et al. (2009); Algahtani (2011); Kotsilieris & Dimopoulou (2013); Coman et al. (2020); Choudhury& Pattnaik (2020); Nissa & Dheanti (2021); Bubou & Job (2021); Khuluqo et al. (2021); Sharifov et al. (2021); Mukumba & Shambira (2022); Sundeen & Kalos (2022)
Cybersecurity Perspectives	An attempt to protect the use of cyberspace against any cyber-attacks. Prevent damage. Being protected from unauthorized access. Addressing any potential threats to information assets in cyberspace.	Lezzi et al. (2018); Kimani et al. (2019); Srinivas et al. (2019); Li & Liu (2021); Perwej et al. (2021); Yusuf & Awoyemi (2022)

Table 1 Continued

Term / Concept	**Description**	**Reference**
Privacy Concerns	The state of keeping data and information protected from any unwanted access, view, modification, or change. Ownership and locality of sensitive identifiable information.	Yang et al. (2020); Alwarafy et al. (2020); Makhdoom et al. (2020); Tabrizchi et al. (2020); Mothukuri et al. (2021)
Cybersecurity Awareness	Being knowledgeable and aware of cyber-attacks and crimes in cyberspace. Know-how to react to cyber threats. Being responsible toward personal safety in the cyberspace. Being aware of malicious activities that are performed by unethical hackers	Modiba et al. (2019); Raj & Nayak (2020); Vaswani (2021); Pyke et al. (2021); Trim & Lee (2021); Zwilling et al. (2022)
Computer Self-Efficacy (CSE)	The ability and confidence of using computer technology. The possession of basic and advanced computer skills.	Ertmer et al. (1994); Zhang & Espinoza (1998); Khorrami-Arani (2001); Paraskeva et al. (2008); Isman & Celikli (2009); He & Freeman (2010); Achim & Al Kassim (2015); Schlebusch (2018); Kwon et al. (2019); Dong et al. (2020); Šabić et al. (2022)
Academic Integrity Concerns (AI)	A type of academic misconduct through which students practice unethical behaviors such as using unauthorized information to complete an exam or assignment.	Casey et al. (2018); Tabsh et al. (2019); Makarova (2019); Burgason et al. (2019); Guerrero-Dib et al. (2020); Ahmad et al. (2020); Ampuni et al. (2020); Arshad et al. (2021); Blau et al. (2021)
Intention to Use (ITU)	The students' willingness to use e-learning platforms in the next semesters / future.	Mailizar et al. (2021); Alassafi (2022)

Research Questions

1. To what extent do *cybersecurity perspectives* affect student's intention to use e-learning platforms?
2. To what extent do students' *privacy concerns* affect their intention to use e-learning platforms?
3. To what extent does students' *cybersecurity awareness* affect their intention to use e-learning platforms?
4. To what extent do *academic integrity* concerns affect students' intention to use e-learning platforms?
5. To what extent does students' *computer self-efficacy* affect their intention to use e-learning platforms?

Priori Hypotheses

- Ha$_1$ Students' cybersecurity perspectives will have significant positive correlation with their intention to use e-learning platforms.

- H0$_1$: *Students' cybersecurity perspectives will not have significant positive correlation with their intention to use e-learning platforms.*

- Ha$_2$: Students' privacy concerns will have significant negative correlation with their intention to use e-learning platforms.

- H0$_2$: *Students' privacy concerns will not have significant negative correlation with their intention to use e-learning platforms.*

- Ha$_3$: Cybersecurity awareness will have significant positive correlation with students' intention to adopt e-learning platforms.

- H0$_3$*: Cybersecurity awareness will not have significant positive correlation with students' intention to adopt e-learning platforms.*

- Ha$_4$: Academic integrity concerns will have significant negative correlation with students' intention to adopt e-learning platforms.

- H0$_4$: *Academic integrity concerns will not have significant negative correlation with students' intention to adopt e-learning platforms.*

- Ha_5: Computer self-efficacy will have significant positive correlation with students' intention to adopt e-learning platforms.
- $H0_5$: *Computer self-efficacy will not have significant positive correlation with students' intention to adopt e-learning platforms.*

Study Limitations

The study had the following limitations: First, there was a limitation related to reaching the desired sample size, since it was impossible to contact all of the selected participants to fill in the questionnaire. Despite the assistance of the Human Review Office in distributing the link of the online questionnaire for this study, there was a delay in receiving answered questionnaires because of the low response of participants. Second, due to the time constraints of the dissertation project, there exists a deadline for submitting the final draft to the committee members and the revised copy to the graduate school. Consequently, several additional research questions were omitted from this dissertation, including a comparison of the e-learning platform (Canvas) utilized at Eastern Michigan University (EMU) with other platforms like Moodle or Blackboard. These comparisons among e-learning platforms can be explored in future research endeavors. Finally, uncertainty was a focal factor that should be considered. Many consequences may occur during conducting this study which may affect the progress and intended objectives for this study.

Study Delimitations

This study was limited to selecting graduate and undergraduate students at EMU as the main sample for the study and excluded students from other colleges or universities. This study did not cover the target of studying students' academic achievement. It was conducted to measure students' intention to use the e-learning platforms within the context of cybersecurity. In addition, this dissertation studied only the five proposed factors of cybersecurity perspectives, privacy concerns, AI concerns, cybersecurity awareness, and CSE. This research excluded studying any other variables such as technology access and attitudes. Technology access is considered an external variable in TAM. Unfortunately, it was complicated to include this variable in the proposed framework for this study. Attitude was another variable that was excluded from this study because of the time restrictions, the need to comply with dissertation requirements, as well as the ability to explain and answer all mentioned questions in this dissertation work.

Study Assumptions

The researcher assumed the participants were truthful and honest when voluntarily responding to the survey questions. Sincerity is important for data collection since getting more precise data means more accurate findings and valid conclusions.

Summary of Chapter One

The purpose of this dissertation was to examine the effect of cybersecurity perspectives, cybersecurity awareness, privacy, CSE, and AI concerns on students' intention to use e-learning platforms. The COVID-19 pandemic affected the learning process and forced the educational institutions to switch to online learning platforms. Access to the learning content on such platforms requires the equal availability of the information and communication technology between students to assure that all students will benefit from online learning features. The point of conducting this dissertation work was to explore students' intention to use e-learning platforms from cybersecurity perspectives without any forcing conditions based on the five proposed predictors for this study.

Chapter Two: Literature Review

Introduction

With the emergence of advanced technology, higher academic institutions are increasingly offering online courses, even complete programs using e-learning platforms. The number of students enrolling into online courses continues to grow in higher education institutions. Especially during the COVID-19 pandemic, many colleges and universities have switched the in-person classes to fully e-learning classes to avoid transmitting the virus. During COVID, this measure stemmed from social distance rules set by the World Health Organization (WHO, 2020). This transition to e-learning was unplanned for many educational institutions. As a result, not all institutions had a smooth transition, especially those that had not previously adopted e-learning platforms (Alqahtani & Rajkhan, 2020). The limited time and shortage of e-learning and management systems made the transition more complicated (Adnan & Anwar, 2020).

Several studies have investigated the success factors in the education domain from both instructors' and students' viewpoints for future improvement in the e-learning environment (Alqahtani & Rajkhan, 2020). Although e- learning has many noticeable significant benefits, such as flexibility, convenience, timesaving, and high self-control by learners (Yen, 2020), it is important to address the challenges of cyber security, privacy and academic integrity, in e-assessment. Consequently, it is very important to identify the factors that are related to cybersecurity, privacy and academic integrity concerns that may affect the acceptance of electronic assessment (e-assessment) using e-learning platforms.

E-Learning Overview

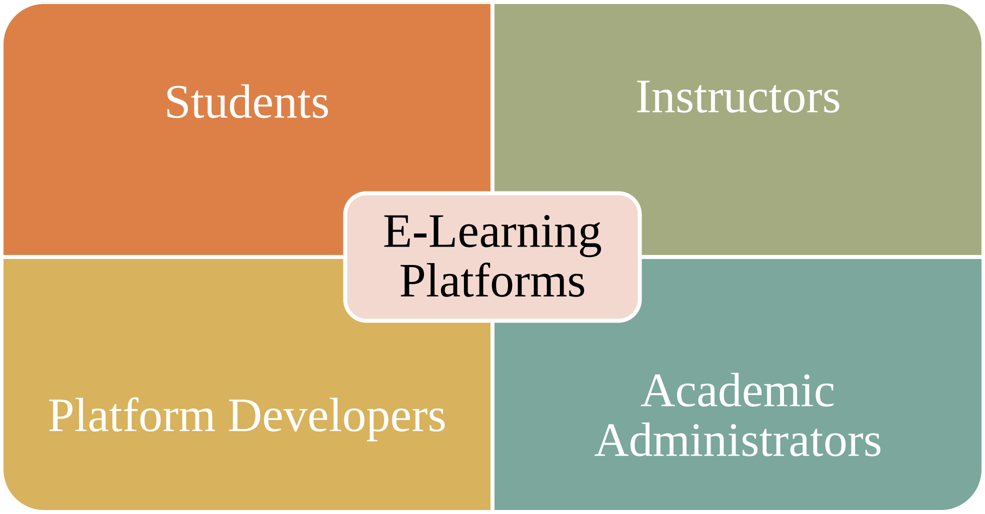
Computer technology has become a crucial component in teaching and learning in academic life at home as well as school, college, or university. The development of information and communication technologies enabled students and faculty to engage in the revolution of e-learning, which can contribute to successful learning processes if the integration of education and technology is assured within the framework of a proper pedagogy (Shamir-Inbal & Blau, 2021).

Distance or remote learning like incorporating social media networks in education (Al-Quraan et al., 2017), online learning, e-learning, virtual learning, web-based education, online education, internet learning, etc. (Agustina & Cheng, 2020) are all terms that represent the education using e-learning platforms. E-learning platforms came to play an integral role in compromising the different forms of electronically mediated learning and teaching. The term of web-based education is defined as the use of internet technology to gain access to web-based courses with the utilization of virtual laboratories and benefits from additional videos with exercises to explain the educational content (Estriegana et al., 2021).

E-learning can take on the forms of synchronous or asynchronous learning. Synchronous e-learning ensures the simultaneous live interaction of learners and educators, which is conducted in the same setting remotely, whereas asynchronous learning provides more flexibility because it does not force students and teachers to meet simultaneously to participate in the learning process (Alquran & Ferdousi, 2022). Communication between the instructor and students could be indirect and reached by electronic processes, such as email messages, threaded discussion posts, or recorded lectures. However, the asynchronous learning process allows learners to access learning materials anytime from anywhere (Hamutoglu et al., 2020; Khalaf et al., 2022). In addition, the learning process can be partially automated and delivered in the mode of hybrid or blended learning, through which the learning process integrates both online and in-person (face-to-face) class activities in an organized systematic way (Proskura & Lytvynova, 2020). See Figure 1 below that was inspired from a study conducted in 2017 (Farid et al., 2017).

Figure 1

E-Learning Access Model



Cybersecurity Overview

Cyber as a term refers to the space of the Internet, and the set of rules that are regulated to protect this space is called cyber security (Bandara et al., 2014). The concept of cyber could be a prefix which points to cyberspace and referred to electronic communication networks and virtual reality (Oxford University Press, 2014). Whereas cybersecurity is defined as an organized set of procedures, resources, processes, and structures that are deployed to maximize the level of protection for both cyberspace and cyberspace-enabled systems from any threats of property rights. It is believed that cybersecurity has three major characteristics that make it different. The first characteristic is its interdisciplinary socio-technical feature, another characteristic was that cyber security is considered to be a scale-free network, in which the capabilities of network actors are potentially broadly similar. Cybersecurity as a term has been released from a belief which assumes that digital space provides absolute freedom for the individuals to do everything they want to do (Alquran & Ferdousi, 2022). There are three factors of cyber-crimes that were derived based on the theory of space transition. Those key indicators of cybercrimes are anonymity, freedom and insecurity (Assarut et a., 2019). For instance, the evolution of the Internet makes it difficult to investigate the incidents of cybercrimes, which facilitate anonymity in the cyberspace especially with the change of the Internet protocol address (Ige, 2020).

The definition and understanding of cybersecurity and its associated risks vary (Alquran & Ferdousi, 2022) with different perspectives and themes to be considered. Strategies for addressing cybersecurity risks also vary, with some favoring a top-down approach focused on controlling cyberspace, while others prioritize protecting security first, leading to a bottom-up approach (Cains et al., 2022).

Security can be defined as the composite of three attributes: confidentiality, integrity, and availability (CIA), which are the core principles of information security (Ferdousi, 2020). These three are the most common attributes that represent the concept of cyber security. Also, the terms such as secure, environ, and asset were crucial to formulating the definition of cyber security (Schatz et al., 2017). Key cybersecurity features were proposed in the National e-learning policy (Buja, 2021). They have claimed that authentication and accountability, access control, and non-repudiation issues have been the serious domains for cyber security in e-learning environments. The function of e-learning platforms has expanded to enable users to communicate with each other, share information and content, and collaborate. As a result, there should be well prepared guidelines and thoroughly studied policies to ensure the protection of the integrity, availability, and confidentiality of information and transactions of data conducted over e-learning platforms (Buja, 2021).

Threats to Cybersecurity in e-Learning Platforms

Trust is the crucial factor for using any digital platform. The researchers explained several types of threats that could occur in e-learning platforms (Bandara et al., 2014). The authors listed the most common risks of online learning environments such as brute force attack, ARP cache poisoning and MITM attack, cross-site scripting (XSS), and cross-site request forgery (CSRF). From another perspective, security and privacy concerns in e-learning are considered ethical risks in the educational process (Mystakidis et al., 2021). Problems that affect e-learning platforms may vary from academic integrity related concerns such as plagiarism, impersonation, and cheating, to include other threats like theft or leakage of questions, and attacks influencing e-exams (Mohammed & Ali, 2022).

Cybersecurity perspectives encompass significant concerns that must be addressed and effectively managed. Within this field, cyber-attacks such as worms, viruses, and macros, as well as acts of theft such as illegal information use and the theft of intellectual property through piracy, infringements, and copyright-related issues, emerge as the primary cybersecurity threats within the context of e-learning platform utilization (Alquran & Ferdousi, 2022). It was concluded that e-learning platforms could be vulnerable to four categories of security threats: authentication, confidentiality, availability, and integrity *(*Rjaibi et al., 2012). The *authentication weaknesses* are represented by the insecure communication which happens if there is a broken authentication or problems with session management. *Confidentiality attacks* can be caused by insecure cryptographic storage and the uncontrolled leakage of information. The denial-of-service attack can cause *availability concerns*. Finally, *integrity attacks* evolve into the inability to restrict URL access, malicious extensions of files, injection flaws, and buffer overflow problems. Other security threats could be caused by unintentional human error or failure such as mistakes made by employees accidentally (Alwi & Fan, 2010). See Table 2 below.

A study revealed if students have not found guaranteed protection, they will hesitate in adopting e-learning systems due to security concerns (Kim, 2021). Security and privacy concerns had negatively affected the ease of participating in e-learning systems; consequently, students will be less motivated to adopt these systems in education (Kim, 2021). Diverse types of cybersecurity issues were organized in groups based on the performing activity (Furnell & Karweni, 2001). For example, security concerns could exist in the enrollment activities that include the registration into courses, establishing authentication parameters, secure payment procedures, and the verification of the selected qualifications. To ensure security, access control to the content, confidentiality, and non-repudiation of communication, and secure the submission of work needed (Kumar & Goyal, 2019). Farid et al. (2017) conducted an exploratory study (inductive research) which aimed to explore the security challenges encountered by e-learning environment in higher education institutions (HEIs) of Pakistan. They coded the main security challenges in e-learning platforms. The researchers (Farid et al., 2017) categorized them into eight patterns including authorization, authentication, privacy, diverse access locations, availability, confidentiality, non-repudiation, and integrity. The study recommended a set of security measures to be applied on e-learning systems. The measures evolved the session authentication, SMS authentication, access controls, biometric authentication, cryptography, secure socket layer (SSL), and physical security devices.

Table 2

Cybersecurity Requirements in e-Learning

Cybersecurity Requirement	Description	Reference
Confidentiality	keeping data private and secret against any illegal access or view. Main attacks in this group of requirements are packet sniffing and session hijacking. In addition, confidentiality attacks include insecure cryptographic storage, insecure direct object references, and improper error handling.	Eibl (2009); Zhao et al. (2010); Bandara et al. (2014); Farid et al. (2017); Sloan & Warner (2017); Srinivas et al. (2019); Prabha & Saraswathi (2020); Tao et al. (2022); Wu et al. (2022)
Integrity	Keeping information safe from unauthorized alteration to ensure consistency. Not only phishing, social engineering, web server vulnerabilities, hardware and software vulnerabilities, and backdoors are the attacks that violate the integrity requirement. But also, buffer overflow, cross site request forgery, cross site scripting; failure to restrict URL access, injection flaws, malicious file execution.	Workman et al. (2008); McCallister (2010); Bandara et al. (2014); Farid et al. (2017); Sloan & Warner (2017); Srinivas et al. (2019); Prabha & Saraswathi (2020); Makhdoom et al. (2020); Zhang et al. (2022)
Availability	Ensure that authorized users have access to the information and systems. Main attacks in this group of requirements are denial of service (DoS) and distributed denial of service (DDoS).	Swanson & Guttman (1996); Ward & Smith (2002); Bandara et al. (2014); Farid et al. (2017); Sloan & Warner (2017); Srinivas et al. (2019); Nguyen et al. (2019); Qiu et al. (2020); Ibrahim et al. (2020); Al Bashaireh (2023)

Table 2 Continued

Cybersecurity Requirement	Description	Reference
Authentication	It is the process of verifying the user's identity to be authorized. Password cracking is one the main attacks occur during the authentication process as well as broken authentication and session management, insecure communication.	Bandara et al. (2014); Farid et al. (2017); Sloan & Warner (2017); Malik et al. (2018); Srinivas et al. (2019); Khan & Alotaibi (2020); Khlifi (2020); Esposito et al. (2021); Banes & Ravariu (2022)
Authorization	The possession of authority, access rights, and permission to perform an activity.	Farid et al. (2017); Srinivas et al. (2019); Kanimozhi et al. (2019)
Non-Repudiation	The principle of non-repudiation stipulates that the sender and recipient of information are required to provide proof of delivery and identification, so that neither can later deny processing the information.	Farid et al. (2017); Srinivas et al. (2019); Mardon et al. (2021).

It is important to quantify the perceived cybersecurity level and the involved risk. For this purpose, the study proposed a predictive functional level security risk management model to be implemented in any cybersecurity context. The model used in research was also used to measure the value of cybersecurity in the e-learning platform. The proposed model aided the cybersecurity specialists in developing safe and secure platforms from the early phases of the system's development (Rjaibi & Rabai, 2018). Cybersecurity threats can be insecure communications, insecure direct object reference, insecure cryptographic storage, denial of service, buffer overflow, injection flaws, malicious file extension, cross site scripting (Upadhyay & Sampalli, 2020), broken authentication and session management, information leakage, and failure to restrict URL access (Alexei & Alexei, 2021). Table 3 below explains more threats.

Table 3

Cybersecurity Threat Category in e-Learning Platforms

Cybersecurity Threat/Category	Description/Examples	Reference
Deliberate software attacks	Attacks occur in form of an infectious programs such as Worms, Virus, Trojan horse denial of service attacks.	Whitman (2003); Alwi & Fan (2010); Romansky & Noninska (2015); Chopra & Chopra (2016); Srinivas et al. (2019); Ibrahim et al. (2020); Perwej et al. (2021); Kumar & Tandon (2022).
Deliberate acts of espionage or trespass	unauthorized access and/or data collection	Whitman (2003); Alwi & Fan (2010); Chopra & Chopra (2016); Romansky & Noninska (2015); Ibrahim et al. (2020); Perwej et al. (2021); Kumar & Tandon (2022).
Deliberate acts of sabotage or vandalism	destruction of information or system	Whitman (2003); Alwi & Fan (2010); Romansky & Noninska (2015); Chopra & Chopra (2016); Ibrahim et al. (2020); Kumar & Tandon (2022).
Technical software or hardware failure and errors	Errors related to bugs and coding problems or those connected to the failures in equipment.	Whitman (2003); Alwi & Fan (2010); Romansky & Noninska (2015); Chopra & Chopra (2016); Srinivas et al. (2019); Ibrahim et al. (2020); Perwej et al. (2021); Kumar & Tandon (2022).
Compromises to intellectual property	piracy, copyright, infringement	Whitman (2003); Alwi & Fan (2010); Romansky & Noninska (2015); Chopra & Chopra (2016); Srinivas et al. (2019); Ibrahim et al. (2020); Kumar & Tandon (2022).
Human error	Mistakes or accidents resulted unintentionally	Whitman (2003); Alwi & Fan (2010); Romansky & Noninska (2015); Chopra & Chopra (2016); Srinivas et al. (2019); Ibrahim et al. (2020); Kumar & Tandon (2022).
Deliberate acts of theft	Confiscation of information or equipment without authorization	Romansky & Noninska (2015); Chopra & Chopra (2016); Srinivas et al. (2019); Ibrahim et al. (2020), Kumar & Tandon (2022).

e-Assessment Overview

Electronic assessment (e-assessment) is the utilization of information and communication technology to create, distribute and grade students' answers and correct their assignments electronically. Two types of assessments can be applied, the summative and formative assessments (Astalini et al., 2019). Formative assignments are prepared to measure students' knowledge and progress during the learning process such as with projects and research papers, whereas the summative type is focused on evaluating the students' understanding at the end of the course or after completing a particular number of chapters, like the required quizzes or tests conducted during or at the end of the course (Khdour, 2020).

Most of the security concerns are addressed in the e-assessment in the e-learning platforms. The verification of identities of students has become the dominant challenge during the assessment process and after the submission of assignments. It becomes difficult to recognize who has had the assessment in the online learning environment. From another side, students need to be authenticated to participate in the learning process conveniently as well, which will create new other challenges related to security protection (Khlifi & El-Sabagh, 2017) and transparency concerns in e-learning (Ismael & Ameen, 2022). The security of e-assessment in the online learning environment is strongly affected by the academic integrity risks which may lead to unfair evaluation of students who adopt e-learning platforms. Two integrity approaches are recommended to mitigate the influence of academic dishonesty, preventive and detective strategies are supposed to be applied in response for this issue (Garg & Goel, 2022). Detective controls can be the usage of online resources, search engines, or any useful software assisting in detecting plagiarism issues, whereas the preventive controls can start with creating an assessment in a form in which the responses of a particular question are distinct to students and can’t be copied (Bujaki et al., 2019).

e-Assessment and Cybersecurity

The e-assessment, which allows learners to receive feedback from instructors instantly and individually, has been applied as a supportive tool in web-based learning in higher education. Consequently, e-assessment assists students to accomplish their work efficiently and improve their performance in class (Huda et al., 2020). E-assessment involves online submissions of homework assignments and grading. However, recognizing the identity of students as well as the authorship of their work submitted online would be considered a serious concern from cybersecurity perspectives in higher education (Okada et al., 2019). Therefore, this study aimed to examine the level of trust regarding the use of e-assessment tools such as TeSLA; this instrument is utilized as an adaptive trust-based e-assessment system (Okada et al., 2019). The study found that factors like accessibility, security, privacy, trust, and the design and feedback of e-assessment are key indicators to assess the effectiveness of e-assessment tools. The proposed factors were categorized into three basic groups: technological, organizational and pedagogical clusters. On the other side, utilizing TeSLA as a trust-based tool to assure safe remote exams will require the installation of dedicated software on learners’ devices, asking to execute multitasks applications during the exam, which may lead to raise learners’ stress and affect their scores negatively.

Privacy Concerns

Privacy is considered the most critical issue linked to the safeguarding of personal transactions of data that are conducted over the internet and related to limiting access to the personal information of users (Husain & Budiyantara, 2020). This study revealed that controlling both privacy and security factors has significantly enhanced the use of e-learning systems. If the privacy level is low in protecting personal data, the satisfaction level could be low, which could lead to a negative attitude toward the adoption of e-learning platforms. In turn, attitude and behavioral intention can play the role of intervening variables to determine the size of effect for the privacy and security on the use of e-learning systems. See Table 4 below.

The adoption of an e-learning environment, especially during the COVID-19 pandemic has emerged privacy concerns, especially in most Muslim countries with conservative cultures (El Andaloussi et al., 2022). Using the theory of social identity, a study found that privacy concerns in this situation are related to social and cultural norms (El-Bassiouny & El-Bassiouny, 2020). A study (Luppicini & Walabe, 2021) has recently conducted a qualitative research work to explore the impact of socio-cultural aspects of e-learning delivery in Saudi Arabia. The study found that both culture and gender gap affect students access to e-learning platforms. It also was demonstrated that the open access in e-learning systems raised the threats to security and privacy. In their study in this regard, Almaiah et al. (2020) have classified the observed contributing factors from the analysis of collected data into two categories. The first category was related to factors such as trust, technological issues, cultural aspects, self-efficacy, and quality concerns, while the second category evolved on financial support, change in management, and technical issues. Privacy and security are treated as the most important aspects in an e-learning environment that should be addressed to guarantee the successful use of e-learning platforms (Kacurova et al., 2021). Highlighting on the data privacy protection while using Zoom platforms, a study suggested various procedures to assure confidentiality such as utilizing an effective use of the waiting rooms in Zoom, admitting students individually when joining the session, and using passwords for validation purposes (Turnbull et al., 2021).

Table 4

Cybersecurity & Privacy Concerns in e-Learning Platforms

Author	Method	Sample	Constructs	Findings
El Tantawi et al. (2015)	Questionnaire	Postgraduate (35) and undergraduate (250) students	Age, gender, grade from last year, computer skills, using computers at home, and frequency of using computers and internet.	There was a positive impact regarding the security and reliability when using e-assessment within e-courses, through which e-assessment can be utilized for large size classes with limited recourses and least costs. On the other hand, there were negative perceptions toward many technical issues and stress related concerns.
Farid et al. (2017)	Exploratory study (inductive research)		Authorization, authentication, privacy, diverse access locations, availability, confidentiality, non-repudiation, and integrity.	The study induced and coded the main security challenges in e-learning platforms in eight patterns (constructs). In addition, the researchers explained many security measures to applied in e-learning such as session authentication, SMS authentication, access controls, biometric authentication, cryptography, secure socket layer (SSL), and physical security devices.

Table 4 Continued

Author	Method	Sample	Construct	Findings
Assarut et al. (2019)	Survey - Questionnaire with closed ended questions.	487 respondents	Freedom, Anonymity, and Insecurity.	The study found that Anonymity and freedom are the key indicators to predict cybercrimes.
Husain & Budiyantara (2020)	Adopted the theory of planned behavior (TPB) and used a questionnaire to collect data.	80 college students.	Security and privacy control, attitude, and intention to use.	The results showed that the control of security and privacy factors had successfully influenced the attitude regarding e-learning use. Attitude and behavioral intention variables were moderators which affected the relationship between security and privacy control and intention to use e-learning systems.
Huda et al. (2020)	Survey-Questionnaire with closed ended questions	200 undergraduate and postgraduate students	Affective Factors, Validity, Practicality, Reliability, Security, and Teaching and Learning	e-Assessment was accepted by students with the expectation that it would be a part of higher education in the future. Approximately 37.5% of respondents agreed that online assessment provides more reliable and accurate results. In addition, students believed that online assessment is as secure as the paper-based exams. However, students found that online exams have more chances for students to cheat.

Table 4 Continued

Author	Method	Sample	Constructs	Findings
Langenfeld (2020)	Literature based review	Related academic articles	E-assessment has involved many issues that need consideration: security and authentication (identity of test taker), privacy, proctored assessment, design of assessment, equity in assessment.	Security concerns in e-assessment are connected to privacy issues that students were anxious for such as, the observation of the test takers in the online based-assessment, the use of personal identifiable information about students, storing the recorded video of the test takers, and sharing their personal data to the host server as well as applying the forensic analysis on their information to discover unauthorized behaviors. In addition, effective e-assessment requires meeting three major conditions, such as: reliable internet connection, accessible content, and appropriate electronic devices.
Dawson (2020)	Book chapter	Related academic articles	Security, privacy, e-cheating, and academic integrity.	The security concerns in e-learning would result in serious problems related to online cheating and academic integrity issues. The author illustrated four security related points regarding e-assessment: unauthorized access to unauthorized data, cognitive offloading for a specific tool, asking others to accomplish the assignment, and disrupting the assessment process.
Almaiah et al. (2020)	Interview using NVivo software.	30 students and 31 experts in e-learning.	Trust, self-efficacy, quality of e-learning, cultural aspect, technological factors, financial support, and change management.	The stratified variables were classified into two groups, the factors influencing usage of e-learning and challenges in the e-learning environment.

Table 4 Continued

Author	Method	Sample	Constructs	Findings
Lara et al. (2020)	Systematic review	10 Related articles	This study shined the light on the importance of techniques in detecting assessment issues in e-learning. Gamifications, block chain, and process mining are good tools to focus on in this area.	Assessment of the e-learning process should be assigned more attention especially in the major of data science. Social network analysis, gamification strategies, and knowledge evaluation have been the areas that need frequent assessment in learning.
Husain & Budiyantara (2020)	Adopted the theory of planned behavior (TPB) and used a questionnaire to collect data.	80 college students.	Security and privacy control, attitude, and intention to use.	The results showed that the control of security and privacy factors had successfully influenced the attitude regarding e-learning use. Attitude and behavioral intention variables were moderators which affected the relationship between security and privacy control and intention to use e-learning systems.
Maatuk et al. (2022)	Questionnaire	135 students and 20 teaching staff	Extent of use e-learning, advantages, disadvantages, and obstacles.	Both teachers and students agreed that e-learning has developed their technological skill as a good point, while increasing the burden from the student side was a negative impact. The obstacles were the lack of financial resources and support, internet connection, the necessity for training, and copyright issues.
Buja (2021)	Exploratory Research	Review of DePAN 1.0 and DePAN 2.0 policies	Authentication & accountability, control of access, protection of communication, and non-repudiation features were proposed.	The proposed features went well with the suggested features for cybersecurity (Infrastructure & Infostructure, e-content, and Governance).

Table 4 Continued

Author	Method	Sample	Constructs	Findings
Tomczyk & Walker (2021)	Focus group Interview-document analysis	Different thousand posts	Technical problems, digital natives or digital competence among students, and the transparency of assessment or the actual involvement of students in the class.	The need to consider digital natives, skills, and knowledge in the online learning platforms.
Paris et al. (2022)	Qualitative systematic research	10 EdTeches platforms	Privacy in e-learning systems.	Platforms such as Canvas and Lu embedded privacy concerns like consent and ownership of student-instructor data. Universities need to negotiate with vendors before purchasing educational software to ensure its compliance with students and instructors' rights to protect their privacy.
Okada et al. (2019)	Mixed Method Research (survey and interview)	108 teaching staff	Concerns of technological (usability), organizational (security, privacy, trust, and accessibility), and pedagogical (assessment).	The used constructs (instruments) were useful to clarify the basics for the e-authentication and authorship verification in e-learning. Five Biometrical and two textual analysis instruments were applied to enhance the e-assessment systems. They were face recognition, voice recognition, keystroke dynamics, face and voice presentation attack detection, plagiarism detection, and forensic analysis respectively.

Cybersecurity Awareness Among Students

Understanding the problem, determining the size of effect, and identifying the reasons causing the problem will mitigate the negative impact on adopting a new technology. Personality traits such as impulsivity, risk taking, and lack of thinking about future consequences of actions are important factors that could be associated with a lack of compliance with cyber and network security policies (Moustafa et al., 2021). In addition, a weak culture of cybersecurity as well as inadequate knowledge to be aware of the impact of cybercrimes have made it easy to engage in suspicious activities (Yusif & Hafeez-Baig, 2021). Therefore, academic institutions must have a cybersecurity policy and strategy that will make students comply with that policy. For instance, Ali & Zafar (2017) developed their model based on Clark et al. (2009) included security and privacy factors of e-learning. The objective of the study to present a conceptual model that focused on some of the information security and privacy factors related to e-learning. They investigated the factors of data evaluation, risk analysis, training, integration, policies, regulations, and architecture in their proposed conceptual framework. See Table 5.

The awareness of cybersecurity among students is an urgent necessity, especially with the increasing number of students that are learning online using information and communication technology in higher learning institutions (Udroiu, 2018). They also need to enhance security levels to be aware of and protected against any potential security threats (Mai & Tick, 2021). For example, passwords security, social engineering activities, malware, and online scam behaviors can be utilized as dimensions to assess students' levels of awareness among various characteristics. It was revealed that many students have an inadequate knowledge and awareness about cybersecurity challenges. As a result, students need proper training and education in this regard. The training sessions with an elaborate explanation of both security content and environment can make them aware of cybersecurity threats and how to prepare themselves to prevent it (Beuran et al., 2019). Cybersecurity training is supposed to be held to serve the goal of disseminating sufficient awareness in this regard (Mai & Tick, 2021). The students in colleges and universities have a good knowledge about cybersecurity concepts, but often they do not comply with the policy to protect their devices (Taha & Dahabiyeh, 2021).

Table 5

Cybersecurity Awareness

Author	**Method**	**Sample**	**Aware Student or Developer?**	**Recommendations/Findings**
Tirumala & Shahamiri (2016)	Survey	2214 students whose ages ranged between 8 & 21 years old.	Students – Not aware enough.	The exponential increase in relying on the Internet and the emergence of bring your own device (BYOD) initiative into education have made it necessary to ensure that students are knowledgeable about cyber security terms, especially those who use smartphones and tablets in online learning. This study recommended developing certain programs aimed to provide awareness for the education curriculum.
Espinha Gasiba et al. (2020)	Different 3 surveys	71 players	Industry (Software developers) - No	The study introduced a platform called Sifu (game - based) which enabled to increase cyber security challenges awareness by performing an automatic evaluation of challenges in compliance to secure coding guidelines due to the lack of software developers' awareness.
Taha & Dahabiyeh (2021)	Online Survey	815 students from all levels	Students - Yes	Training Sessions and campaigns are needed to spread awareness.

Table 5 Continued

Author	**Method**	**Sample**	**Aware Student or Developer?**	**Recommendations/ Findings**
Zhang-Kennedy & Chiasson (2021)	Comprehens_ive systematic review	All relevant academic publications from the past 20 years about the information security awareness and education area	------	The review organized 119 needed multimedia tools to educate users about cybersecurity into five categories: digital games, film and animation, tabletop games, learning modules, and comics.
Mai & Tick (2021)	Questionnai_res/Quantitative analysis	313 participants	Students - No	Use psychological methods to improve awareness and comply with information security policies.

Table 5 Continued

Author	Method	Sample	Aware Student or Developer?	Recommendations/ Findings
Wahid (2021)	Online survey - questionnaire	300 samples	Enhance National e-learning policy.	Adopt and utilize Information Security Awareness Model which is dedicated to providing an awareness-oriented cybersecurity education model. Awareness of information and cyber security could be summarized in five dimensions of perceived vulnerability, severity, self-efficacy, response efficacy and cost. These dimensions were significantly predicting the intended behavior.
Corallo et al. (2022)	Systematic literature review	Deep review of 23 related academic articles served the purpose of this study.	Organize and summarize the most important definitions of cybersecurity as well as recognizing the most commonly used techniques to disseminate awareness in this topic (information & cyber security). Finally, this study clarified the perceived benefits obtained from awareness.	Awareness of cybersecurity would achieve the following advantages, the ability to predict cyber-attacks, prevent them, reduce the probability of occurring any potential attacks, empower the existing infrastructure, and improve the effectiveness of employees in responding to the occurred attack and know-how to behave in regard to any similar situations.

Academic Integrity in E-Learning

Academic integrity is a big issue that includes academic dishonesty, which can be represented in two basic ways. The first type of academic integrity relates to the educational activities such as research, service, and teaching - these activities are taken on by academics and judged based on their reference to the whole integrity (or lack of it). The second type of academic integrity relates to character or personality such as the set of values, behaviors, and conduct in the educational activities (Macfarlane et al., 2014). Misconduct in academic settings and practices could include many activities that violate the ethical rules and basics. For instance, academic cheating is defined as misconduct that involves unethical practices such as using unauthorized information to complete an exam or assignment. When a student attempts to submit another student's work materials, or a work prepared by another person as his or her own or helps others in getting unauthorized materials, those are examples of cheating (Burgason et al., 2019).

While this unethical practice prevails in the in-person academic settings, in online environments this practice is more possible. Students engaging in academic integrity issues requires the availability of many factors. The opportunity to cheat, the existence of an incentive, and the justification are vocal points that encouraged students to cheat (Alessio et al., 2018). All these factors are more prevalent in the online environment. As a result, cheating among students in online learning environments has been raised. The main reason for this increase was attributed to the adoption of technology in the learning process; technology was identified as providing the source of academic dishonesty (AD). With the assistance of technology, cheating methods or techniques were developed to evolve many times (Mellar et al., 2018). In addition, students are more likely to engage in AD when facing problems like being under stress and pressure, when the norms are unclear, and when there are temptations and opportunities. Academic integrity issues might lead to several ethical risks (Lederman et al., 2020). Many problems related to security, privacy, trust, equity, and dependency could be a huge effect caused by ethical risks raised from academic dishonesty and ethical concerns (Wakunuma & Masika, 2017).

Table 6

Academic Integrity in e-Learning Platforms

Author(s)	Method	Sample	Constructs	Findings
Turnbull et al. (2021)	Integrative review	52 papers review from 4 databases (Ebsco, Gale, Informit, and Proquest)	Technology, pedagogy, and content (TPACK) model.	Academic dishonesty, access to technology, confidentiality and data privacy, online competence, and reconciling synchronous/asynchronous delivery were the major concluded challenges found in e-learning.
Wakunuma & Masika (2017)	Qualitative research - Survey to collect Demographics Data, then using an interview to complete the collection of needed data.	3 information systems (ISs) professionals from African and International countries.	Ethical risks evolve issues related to equity, ownership, dependency, privacy, trust and security	Ethical risks may lead to both unfreedom and capability deprivations which would in turn hinder the development of information and communication technologies (ICTs).
Tomczyk & Walker (2021)	Focus group Interview - document analysis	Different thousand posts	The reliability of students' submitted assignment	It was noticed that online cheating became widespread in digital education that students were not approaching their homework as expected.

Table 6 Continued

Author(s)	Method	Sample	Constructs	Findings
Luppicini & Walabe (2021)	Qualitative research, data collected by interview and thematic analysis.	28 experts in socio-cultural aspects of e-learning delivery in Saudi Arabia	Social and cultural aspects of e-learning. Adopting social identity theory.	The study concluded that two thematic variables were influenced by e-learning use, they were culture and females' access to e-learning and use.
Wiley (2020)	Survey	789 instructors	Cheating and plagiarism in online learning environment	The absence of the physical attendance of students in distance learning has created new forms of cheating such as purchasing solved assignments, copying answers of others, and sharing answers. There should be strict procedures to follow like adopting lockdown browsers during the exams, forcing students to turn on their webcams, and checking plagiarism.
Alier et al. (2021)	Systematic review	Academic articles about privacy in learning management systems (LMS).	The ethical and privacy dimensions	The study linked the ethical part in the learning management systems (LMS) to the data surveillance and privacy concerns. Ethical issues were explained from different points of views which could take the face of students' control over data, security, assessment, and transparency. Ethical and privacy concerns should be discussed socially to be clearly understood according to the different cultures.

Computer Self-Efficacy (CSE)

Compeau and Higgins (1995) defined computer self-efficacy (CSE) as an essential factor to describe the peoples' using computer technology. Supporting this definition of CSE, Ferdousi (2019) illustrated that CSE is a vital indicator which has a significant effect in predicting students' intention to adopt digital technology in the learning process. Aldhahi et al. (2022) have illustrated the impact of computer self-efficacy on satisfaction levels of e-learning. In a study on online learning, online learning self-efficacy (OLSE) was defined as the students' ability to navigate online learning systems, submit assignments on time, communicate with either instructors or technical support team, manage time, and the ability to learn a new technology without the instructor's help. The study was a cross sectional that has deployed a questionnaire to collect data from a sample of 1226 from 22 Saudi Arabian universities. The results revealed a significance of relationship between the selected dimensions of self-efficacy which were represented by technology, time management, and learning. Malli et al. (2021) have found that students in sport science showed no relationship between their self-efficacy and their habit in playing sport or gender, but there was a significant relationship between their self-efficacy and their expectations and readiness for e-learning systems use.

From students' perspectives, the effectiveness of e-learning could be determined by the factors of prior knowledge and the learning style that may affect their self-efficacy. Azis and Leatemia (2021) have demonstrated that students with visual learning style would have a high computer self-efficacy, which has influenced their learning outcomes. While students with low self-efficacy are discouraged by failure. They assume failure relates to their inadequate abilities to perform tasks. Therefore, this type of students usually avoids taking any difficult tasks. On the other hand, from the instructors' perspectives, a study surveyed by Chibisa et al. (2021) to examine the factors that may affect their computer self-efficacy, revealed that social and demographic influence, ease of use, usefulness, basic computer skills, actual computer use, and access to computer technology were significantly associated with computer self-efficacy by 73.7% variance.

Self-efficacy is also associated with the interpersonal relationships that are needed in the e-learning environment. Kong et al. (2021) have asserted that self-efficacy has a significant role in impacting interpersonal relationships positively. The study clarified that self-efficacy could be reflected in people's motivation, cognitive, or emotional effects. Researchers have explained the correlation between interpersonal relationships and self-efficacy through the necessity of encouraging students to communicate with each other to solve problems, build trust, and think critically. This way, students would learn the skills of self-management as well as self-awareness. Mapuva (2009) demonstrated that the lack of confidence in using the technology and how to interact with the instructor over the online learning platforms had been raised to be essential concerns that need to be addressed. See Table 7 below.

Table 7

Computer Self-Efficacy (CSE) Concerns in e-Learning Platforms

Author	Method	Sample	Constructs	Findings
Ferdousi (2019)	e-Survey	94 Students	Attitude and Computer self-efficacy (CSE).	Both CSE and Attitude have had a significant impact in determining Acceptance of technology.
Kong et al. (2021)	Experimental study	214 students	Exploratory education, self-efficacy, interpersonal relationship.	Results revealed that exploratory education has influenced both self-efficacy and interpersonal relationships. In addition, self-efficacy has a significant positive effect on interpersonal relationships.

Table 7 Continued

Author	**Method**	**Sample**	**Constructs**	**Findings**
Talosa et al. (2021)	Qualitative research – interview. This study is based on phenomenology like the perceptions of researchers.	35 students.	Technological self-efficacy and self-regulated learning (self-supervising and self-exploration), personal (time management), interaction, motivation, teacher factor, and home environment.	Technological self-efficacy and self-regulated learning themes were opportunities in e-learning. While other factors acted as challenges emerged in the e-learning environment.
Chibisa et al. (2021)	A 5-point Likert scale questionnaire, it used a technology acceptance model (TAM).	400 pre-service teachers.	Demographics influence, ease of use, usefulness, social influence, basic computer skills, actual computer use, computer self-efficacy, and access to computers.	All independent factors explained a significant impact on computer self-efficacy with high variance.
Okuong _hae et al. (2021)	Survey with closed-ended questionnaire.	320 library and information Science students in Nigeria.	Technology readiness, Computer self-efficacy (CSE), and e-learning adoption.	Both technology readiness and CSE revealed a high correlation with e-learning adoption. Two variables succeed in predicting e-learning adoption, but CSE was stronger than technology readiness in explaining e-learning adoption.

Table 7 Continued

Author	Method	Sample	Constructs	Findings
Chopra & Madan (2021)	Exploratory study	Deployed four major sources of information by Bandura's (1977) theory of self-efficacy.	Potential self-efficacy, and e-learning effectiveness, and using gender as moderator.	It was concluded from the collected responses that there was an indirect impact of e-learning systems on the quality and effectiveness of e-learning by using PSE, also it was stronger for males compared to the females.
Azizi et al. (2022)	Mixed methods study using questionnaire and semi-structured interviews	440 Iranian students.	Computer self-efficacy (CSE) and e-learning anxiety.	Beginning, mainframe, and advanced skills were used as factors to build CSE the basic dimension, it was found that CSE would highly determine the e-learning anxiety. There was a strong negative association between CSE and E-learning anxiety. In addition, new themes were developed like the increased ability to solve problems, improved digital literacy and self-regulated learning, as well as enhanced learning satisfaction.

Table 7 Continued

Author	Method	Sample	Constructs	Findings
Aldhahi et al. (2022)	Cross section study-using questionnaires.	1226 students from 22 Saudi Arabian Universities.	Online-learning satisfaction, and self-efficacy (OLSE).	Time management, learning, and technology were the components of online learning self-efficacy. E-learning satisfaction showed a high relationship with the components of self-efficacy. Since e-learning self-efficacy was a predictor for determining satisfaction.
Sulaymani et al. (2022)	Survey	265 secondary school students.	Computer self-efficacy (CSE), ease of use, gender, social influence, and willingness to use e-learning platforms.	CSE had a positive relationship with older students, while there was a negative relationship with young students. In addition, it was found that CSE and social influence were the major predictors for students' intention to use e-learning systems.
Udin et al. (2022)	Online questionnaire	156 students	Computer self-efficacy (CSE), self-awareness, comfortability, social interaction, instructor's support, and online learning use	CSE impact was represented by the comfortability and self-awareness, they had a positive correlation with the implementation of e-learning platforms. On the other hand, social interaction was insignificant in predicting the students' intention to adopt e-learning platforms.

Table 7 Continued

Author	**Method**	**Sample**	**Constructs**	**Findings**
Meinhardt-Injac & Skowronek (2022)	Survey	159 students	Computer self-efficacy (CSE), computer anxiety, the use of information and communication technology (ICT), and academic performance.	There was an inverse relationship between CSE and computer anxiety. Another result was found that no differences were observed among the multiple groups of students who started or almost finished their Bachelors' degree regarding both computer anxiety and CSE.
Oetomo & Santoso (2022)	Questionnaire	244 students	Internet self-efficacy, quality of lecturer and the information and communication technology (ICT), students' engagement and learning effectiveness.	The factor which had significantly affected the engagement level was the quality of ICT, but not quality of instructor or the internet self-efficacy. Consequently, the engagement variable influenced the effectiveness of learning.
You (2022)	Questionnaire	186 students	Gender, grade, years of using e-learning systems, subjects, behavioral and emotional engagement, cognitive input, self-efficacy, and learning completion.	Emotional, behavioral, and cognitive dimensions significantly determining the degree of learning completion. self -efficacy had partially and positively mediated and impacted the relationship between the online learning engagement and the learning completion. Finally, there was no difference in the learning completion by gender or subject.

Table 7 Continued

Author	Method	Sample	Constructs	Findings
Di Giacomo et al. (2020)	Questionnaire	Computer anxiety, ability to use technology, and technophobia.	117 students	The inadequate management of technology led to technophobia.

Demographics

Gender

In gender schema theory (Bem, 1981) and in other technology acceptance models such as TAM 2 as well as the theory of planned behavior, gender has been incorporated into models of behavior. Previous research revealed that both men and women use different socially constructed cognitive structures when making decisions (Venkatesh & Morris, 2000). According to Venkatesh et al. (2003), gender had a significant impact on the relationship between performance expectancy which acted as a perceived usefulness and behavioral intention toward using any new technology, with men having a significantly stronger relationship than women. Therefore, gender will be included in this study as an independent variable. This research work will attempt to discover any differences among the groups of privacy factor by gender. Chao (2019) used gender, age, experience, and voluntariness of use as moderators that affect the relationships between social influence, effort and performance expectancy, and the behavioral intention to use mobile learning technology.

Ethnicity

Islam et al. (2011) illustrated that there has been a growing need to strengthen information and communication technology frameworks and e-learning in industrialized countries as a means to address the digital divide between those who have access to technology and those who cannot. According to Mungania (2003) reported that 49% of e-learners were “Caucasian” or “White.”

This research work plans to explore the impact of ethnicity on the academic integrity perceptions of students. A number of cultural factors were investigated to determine whether an e-learning system would be accepted by a student, and some significant indications were given regarding the cultural dimensions that should be taken into consideration when implementing an e-learning system in a school (Thowfeek & Jaafar, 2012).

Discipline

It is believed that e-learning would be more useful in IT and engineering subjects (Islam et al., 2011). In a study of behavior intentions to adopt e-learning technology, research found that a scientific discipline is a critical moderating factor (Altameemi & Al-Slehat, 2021). This research work assumes that students from technology related majors have a cybersecurity awareness more than other students who are from different non-technology majors. Consequently, students from technology related backgrounds have the intention to use e-learning platforms more than students who are from non-technology related backgrounds.

Level of Education

According to Claar et al. (2014), a new learning management system's acceptance is investigated based on various demographic factors such as age, race, gender, and education level. It was concluded that level of education shows a significant impact on the perceived usefulness (PU) and perceived ease of use (PEOU). While age was only a predictor of PU. A positive correlation was found between the level of education and PU by Venkatesh et al. (2000). In the same way, Burton-Jones and Hubona (2006) concluded that higher education levels lead to a higher degree of PU and that users with higher levels of education are less sensitive to PEOU due to the reduction of computer anxiety and improvement of attitude.

Theoretical Background of Research Frameworks

Theory of Reasoned Action (TRA)

The theory of reasoned action explains volitional behavior. The scope of this theory excludes a wide range of behaviors. The excluded behaviors vary from those that relate to spontaneous or impulsive behaviors. Furthermore, behaviors that require special skills or opportunities are excluded too (Hale et al., 2002).

Hole et al. (2002) presented a causal framework with complete components that formed the key constructs of TRA. Attitude is predicted by belief strength and belief evaluation, whereas normative beliefs and motivation predict subjective norms, and both attitude and subjective norms are significant predictors of behavioral intention (Park, 2000), which is the explanatory variable for the final volitional behavior (Ajzen & Madden, 1986; Montano & Kasprzyk, 2015).

Planned Behavior Theory (TPB)

Intentions that are associated with certain behaviors could be predicted. Ajzen (1991) demonstrated that the planned behavior theory (TPB) was able to predict the behavior of individuals with a high level of accuracy based on three core components, attitudes toward performing that behavior, subjective norms, and perceived behavioral control. These components combine to form behavioral intentions (BI). TPB aims to link the set of beliefs to behavior. Alleyne and Phillips (2011) demonstrated in their study that TPB is considered an enhanced version of the theory of reasoned action (TRA). Through TPB, TRA's predictability power was improved. TPB was found to be supported by empirical evidence (Ajzen, 1991). However, Manstead (2011) shed light on previous studies that criticized both theories (TRA and TPB) for neglecting social factors. Figure 2 below demonstrates the key constructs that build TRA and PBT models. This figure was inspired from Montano and Kasprzyk (2015).

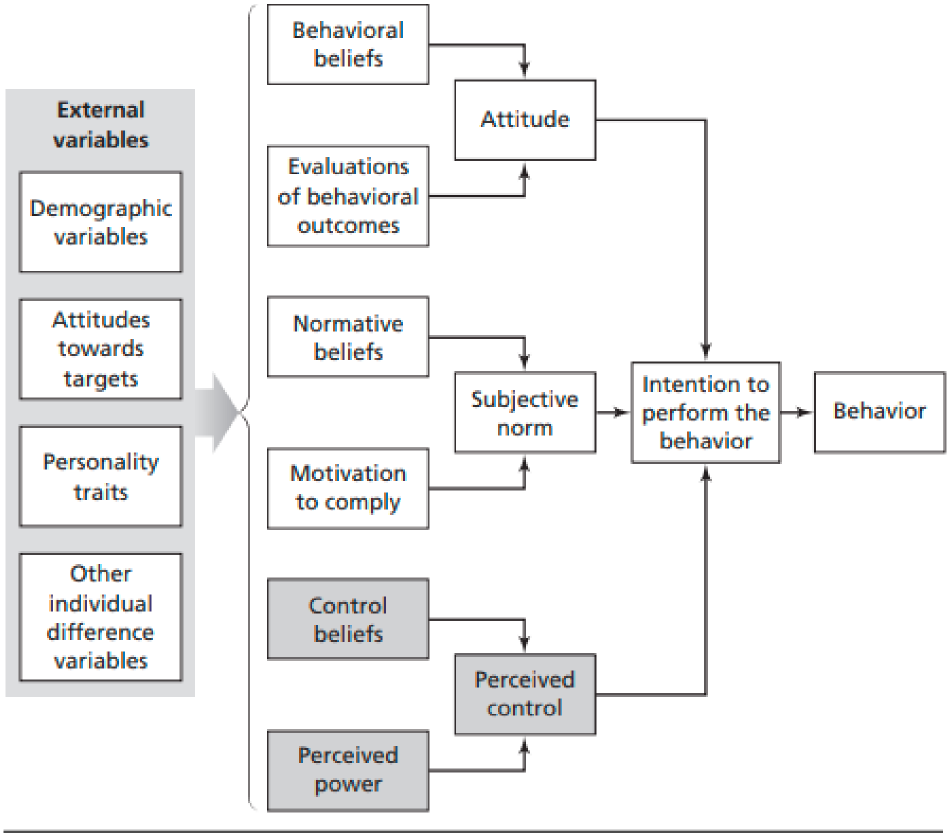
Diffusion of Innovation Theory (DIT)

The diffusion of innovation theory was developed by Rogers in 1962. A diffusion theory was developed in communication to explain how ideas or products diffuse through population groups or social systems over time (Rogers et al., 2014). As a result of this diffusion, people in a social system adopt a new idea, behavior, or product. Adoption is the act of changing what one previously did. In order for ideas, behaviors, or products to be adopted, the person must perceive them as novel or innovative (Singh, 2006).

Gabriel Tarde plotted the original S-shaped diffusion curve in 1903 to illustrate the Diffusion of Innovation Theory (Kaminski, 2011). Lundblad (2003) reviewed Rogere’s DIT by explaining the basic elements that establish this theory to be innovation, communication, time, and the social system together. They acted as the primary elements of Rogers' diffusion of innovation theory which had been proposed in 1955 (Rogers, 1995). Lundblad (2003) clarified that Rogers' diffusion of innovation theory building and research began with, and still primarily focuses on, diffusion and adoption by individuals rather than within organizations.

Figure 2

Theory of Reasoned Action & Planned Behavior Theory



Technology Acceptance Model (TAM)

Technology acceptance model (TAM) has been one of the most influential models of technology acceptance, with two basic constructs influencing an individual's intention to use recent technology (ITU). Both factors are perceived ease of use (PEOU) and perceived usefulness (PU). Fishbein et al. (1980) clarified that the original source of TAM was the theory of reasoned action (TRA). TAM is a model that has been derived from an information system theory. The goal of TAM is to study the behavior that individuals follow regarding the adoption of a particular technology. The intention of users to use a given technology is the essence of

TAM since it measures their behavioral intention (BI) based on their perceptions (or what is known as attitude). It consists of two basic constructs, perceived usefulness (PU) and perceived ease of use (PEU). Davis (1989) is the original version of this model. Using TAM, researchers can examine the impact of moderating variables such as culture, gender, and task (Adams et al., 1992), as well as extend the model with external variables that describe the characteristics of the individual, organization, and task (Lee et al., 2003).

Significance of TAM. TAM is a flexible framework. It can be scalable to include external variables needed to serve the goal or purpose of particular studies. The development of a comprehensive TAM that would be able to examine e-learning acceptance under all circumstances is considered a crucial research area (Salloum et al., 2019). TAM is popular; various sectors have utilized TAM including commerce, health, government, the economy, and education. For example, researchers have deployed TAM in many cases of technology acceptance, such as accepting electronic wallets (e-Wallets). To and Trinh (2021) have used TAM to examine the factors that influenced the adoption of e-wallet technology by incorporating external variables like trust and enjoyment into their study. The same concept has been applied in the study conducted by Prakosa and Sumantika, which reveals consumers' intentions regarding using electronic marketplaces (e-Markets) and the level of trust they have with these systems.

In acceptance of e-learning, TAM has been applied to many situations. For instance, TAM helped in determining the teachers' intention to use online learning platforms during the COVID-19 pandemic (Mailizar, Burg, et al., 2021) as well as the instructors' perceptions regarding the use of e-learning in teaching subjects like Mathematics (Mailizar, Almanthari, et al., 2021) or Physics (Halim et al., 2021). Tawafak et al. (2021) have illustrated with the aid of the TAM model that a massive open online course (MOOC) can be used as an actual system within e-learning platforms. Finally, TAM has been used as an evaluation tool to examine the effectiveness of e-learning systems from many perspectives of educators and learners (Maharani & Usman, 2021; Mohamad et al., 2021).

Strengths & Weaknesses of TAM. TAM has become the dominant framework applied to the study of behavior related to the intention to accept a specific technology in the field of information systems (IS). TAM has built a robust base in the research field; many studies employ it as a methodological approach to guide their experiments or arguments. TAM has been influential and powerful. Davis (1989) established psychometric scales for both constructs PU and PEOU to be widely approved and replicated in various research work through which deployment of these scales strengthens TAM (Chuttur, 2009). In addition, TAM can be used as a general grounding framework (Arbaugh, 2010) and flexibly modified to fit different purposes of variant studies. TAM provides consistent factors that can help investigate adults' intention to adopt new technology (Braun, 2013).

In the e-learning field of study, Ibrahim et al. (2017) adopted TAM to explore the preferences and characteristics of learning in environments whose individuals (students and staff) were reluctant to use online learning technology. TAM was successfully applied and assisted researchers in highlighting the critical issues needed to sustain e-learning systems and improve their effectiveness. See Figures 3, 4 and 5 below. The original TAM below in Figure 3 (Davis, 1989) is commonly known with TAM. Figure 4 is TAM2 which is an extended from the original TAM (Venkatesh, 2000; Venkatesh & Bala, 2008).

TAM has been widely applied in e-commerce adoption studies. Nyoro et al. (2015) reviewed 25 publications in the e-commerce area. These publications utilized TAM as a methodological framework and benefited from its ease of use and flexible features. Although

TAM has many advantages, Nyoro et al. (2015) concluded a critique of TAM based on the conducted review. TAM had imperfections in its embedded relationships and an apparent deviation in the expected results.

There were comprehensive limitations in TAM that had been observed and summarized by Lee et al. (2003). For instance, TAM was criticized for the self-reported usage of technology without measuring the actual usage. In addition, TAM conducts research using a single information system. Therefore, TAM does not reflect the real working environment, and the newly developed measure has low validity and is based on a singular item scale. Finally, TAM fails to demonstrate causality in the model, applies a single task, and relies on a one-time-based cross-sectional study.

Figure 3

Original Technology Acceptance Model

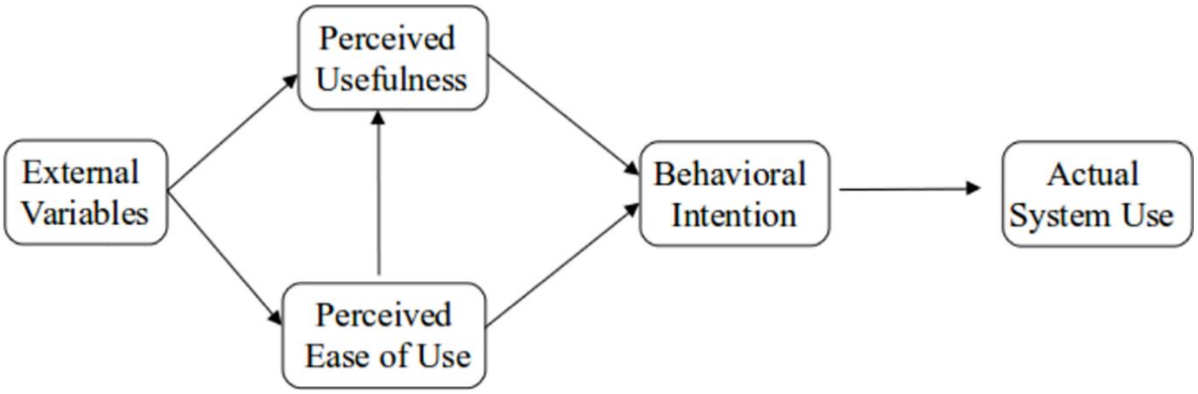


Figure 4

Technology Acceptance Model 2

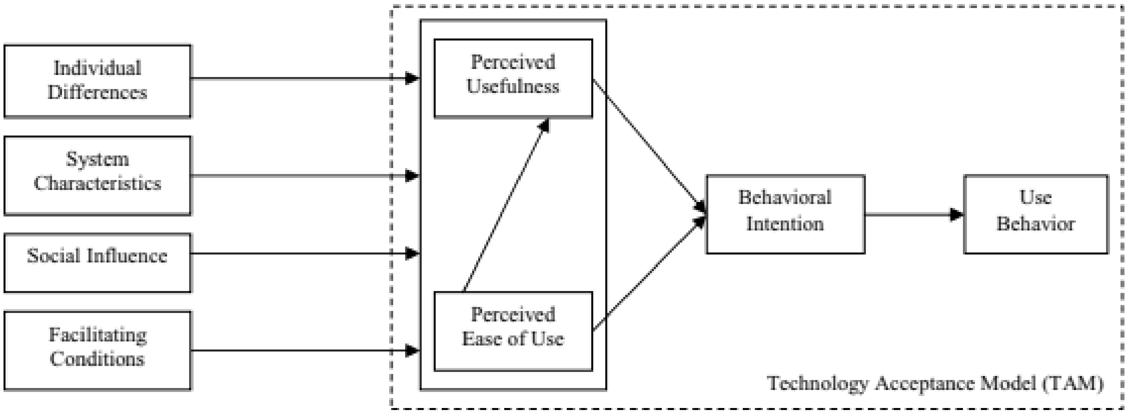
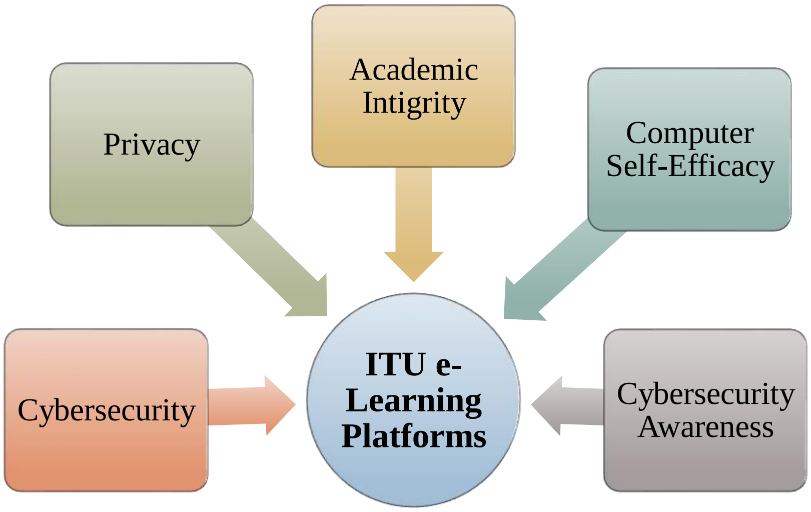


Figure 5

Proposed Conceptual Model of Students' Intention to Use E-Learning Platforms



Applying the Extended TAM 3 in the Proposed Conceptual Model

According to Davis (1989), TAM consists of four basic constructs, namely perceived usefulness (PU), perceived ease of use (PEOU), behavioral intention (BI), and behavior (B). Lee et al. (2003) explained the relationship between PU and PEOU and PU, PEOU, and BI. A significance was approved among these variables. From one side, PEOU successfully predicted PU, and both PU and PEOU were significant predictors for BI.

For this research work, extended TAM 3 (Venkatesh, 2000; Venkatesh & Bala, 2008) is going to be adopted to research and analyze the idea of this dissertation work. See Figure 6 below. This dissertation work assumes that when students have confidence (computer self-efficacy) and enough awareness of cybersecurity threats, they will find it useful to use secure and private platforms for the e-learning process. According to the extended TAM 3, this dissertation work will represent both cybersecurity awareness and computer self-efficacy as variables under the PEOU construct. While cybersecurity, privacy, and academic integrity will represent the PU. As a result, this dissertation work believes that the five proposed factors will affect the intention to use the e-learning platforms. See Figure 7 in the next section.

Figure 6

Technology Acceptance Model 3

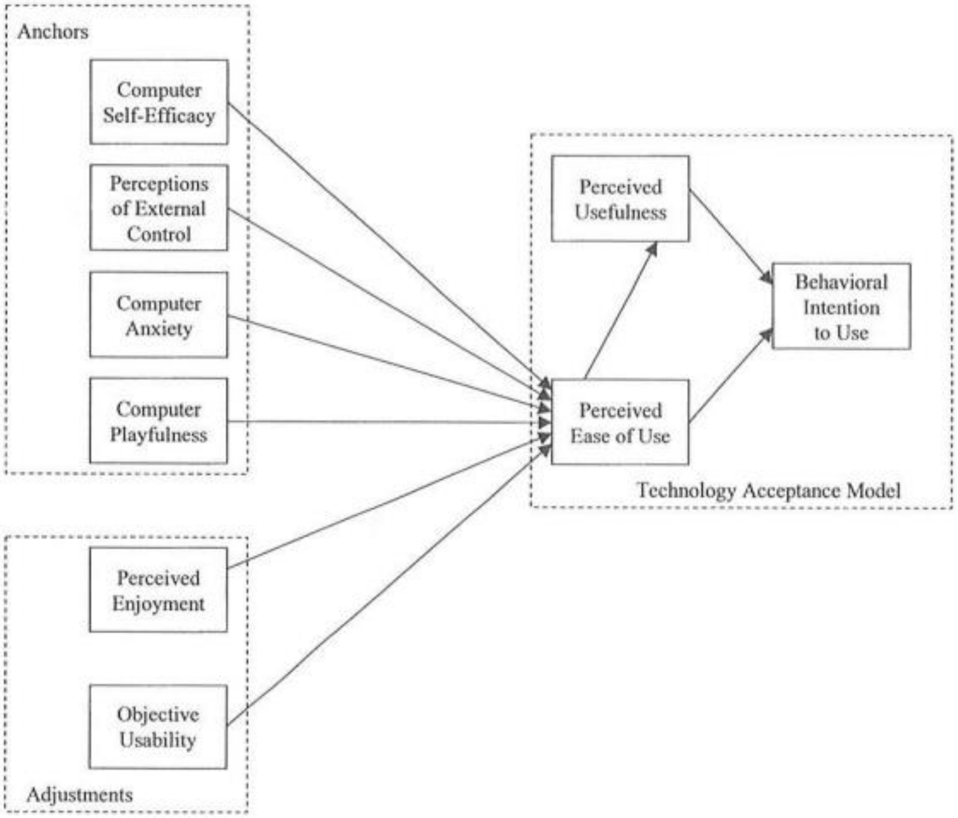
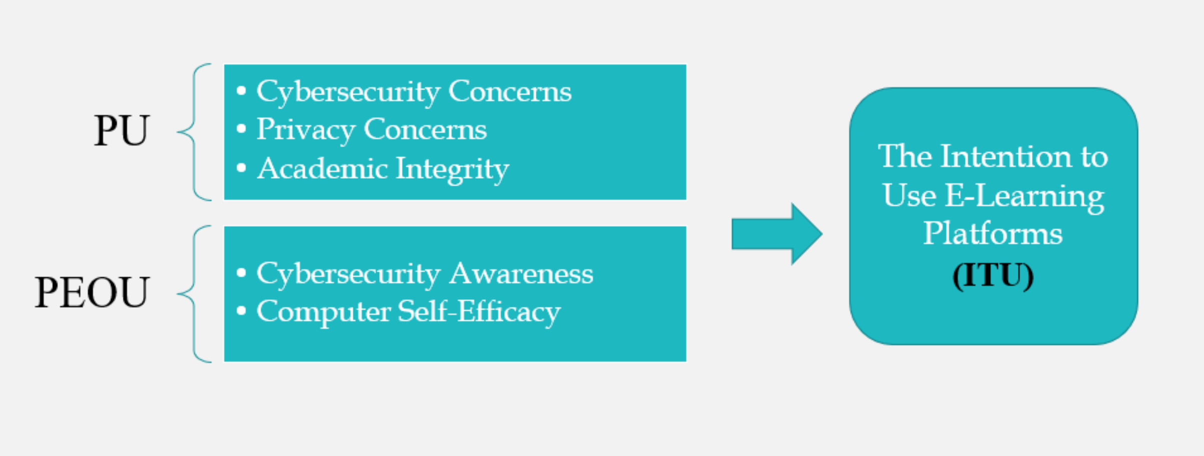


Figure 7

PU & PEOU Variables for This Research Work According TAM3



Note. The perceived usefulness (PU) will include cybersecurity perspectives, privacy concerns, and academic integrity concerns variables, whereas the perceived ease of use (PEOU) will explain computer self-efficacy and cybersecurity awareness.

Theories Adopted in Examining Cybersecurity Risks

Space Transition Theory (STT)

The space transition theory was developed by Jaishankar in order to explain the causation of cybercrime. According to Jaishankar (2007), cybercrimes require a separate theory. Cybercrime was found to be inadequately explained by general theoretical explanations. This theory discusses how individuals behave in physical and cyberspace according to conforming or non-conforming behavior (Li, 2021). The concept of space transition describes movement between spaces (e.g., from the physical realm to the cybersphere and vice versa). When individuals move between different spaces, they behave differently. This is what the theory of space transition argues (Jaishankar, 2007). Researchers around the world have evaluated the applicability of the space transition theory to the four basic categories of cybercrimes.

Consequently, they found that it was more applicable to cyber-trespassing, cyber-deception, and cyber-pornography than cyberviolence (Abayomi, 2020).

According to Jaishankar (2007), there are seven axioms (Abayomi, 2020) of STT:

1. Persons with repressed criminal behavior (in the physical space) are more likely to commit crimes in cyberspace, which they otherwise would not commit in the physical space due to their social standing and position.
2. In cyberspace, identity flexibility, dissociative anonymity, and lack of deterrence factors provide offenders with the option of committing cybercrime
3. Cybercriminals are likely to export their criminal behavior into physical space, which in turn can be exported into cyberspace.
4. Offenders' intermittent ventures into cyberspace and the dynamic spatio-temporal nature of the cyberspace provide a potential escape route.
5. Strangers are likely to collaborate in cyberspace to commit crimes in physical space. Furthermore, in cyberspace, associates from physical space are likely to commit crimes together.
6. Cybercrime is more likely to occur in closed societies than in open societies.
7. Crimes in cyberspace may result from conflicts between physical and cyberspace norms and values.

According to the STT, it is believed that most of threats and attacks which may occur over the e-learning platforms like the unauthorized access of data can be related to one or more of the mentioned above axioms. The researcher believes that using STT in this research will be significant to explain the psychological factors of students toward performing illegal/unethical activities when using the e-learning platforms in cyberspace.

Protection Motivation Theory (PMT)

Protection motivation theory was developed by Rogers in 1975. The purpose of this theory was to provide a better understand the correlation of fear appeals and attitude change (Haag et al., 2021). The theory was concentrated on describing how people are motivated to respond in a self-protective way towards a perceived health risk (Westcott et al., 2017). Threat appraisal and coping appraisal are the two basic constructs that build this theory (Preissner et al., 2022). While threat appraisal focused on the assessments of a persons' vulnerability and the level of severity of a certain threat, coping appraisal clarifies the perception that a recommended activity which can efficiently avoid the threat (for example, response efficacy) as well as the confidence level that a person is being able to engage in the recommended behavior such as self-efficacy. The PMT revealed that people with high efficacy appraisals are more likely to adopt recommendations to minimize the possibility of occurring threats when they evaluate their own susceptibility and the degree of threat's severity to be high (Preissner et al., 2022).

Haag et al. (2021) have applied PMT on the information system (IS) field of study. They reflected the aspects of threat and coping appraisal on how the individuals who use technology such as the internet networks concern regarding their privacy and security assurance, and how they can respond in case of having an attack happens. According to Haag et al. (2021), this theory is included in this dissertation work to investigate the perceptions of students who use the e-learning platforms toward their intention to use these platforms in the future according to the cybersecurity aspects.

Computer Ethics Theory

As digital computers and cybernetics emerged in the 1940s, computer ethics began to develop. Consequently, computer ethics has been explored from different perspectives. These perspectives include computer ethics not being a real discipline, being a pedagogical method, being a unique discipline, being applied ethics, and utilizing information ethics as its foundation. In light of the increasing integration of information and communication technology (ICT) into society, it is necessary to develop foundations for computer ethics. (Charlesworth & Sewry, 2009).

Johnson (1985) explained that certain issues continue to persist in computer technology as it evolves and is deployed in different ways. Privacy issues, rights to property, accountability issues, and issues related to social values are considered serious concerns to address (Jaeger et al., 2008). Ethical issues can be categorized in three different factors: technology type, sector in which the technology is used, and ethical concept (Longo et al., 2020).

Elaborating the most significant aspects related to the ethical issues of cybersecurity. Christen et al. (2020) illustrated that a number of ethical issues arise as a result of cybersecurity, including ethical hacking, dilemmas regarding “zero-day” exploits, balancing the need for access and privacy of sensitive health data, or value conflicts raised by encryption algorithms in law enforcement. Therefore, the computer ethics theory is listed in this research, through which a link of the reasons behind the academic integrity behaviors can be realized and investigated to serve the purpose of this study.

Table 8

Theoretical Models Adopted to Evaluate e-Learning Platforms.

Author	Model/Theory	Constructs	Purpose	Findings
Rahmi et al. (2018)	Technology Acceptance Model (TAM)	Perceived usefulness (PU), perceived ease of use (PEOU), and Intention to use (ITU)	This study had the goal of determining the factors that affect the individuals' intention to use e-learning and to get results which can guide system developers and researchers.	Classify accepted variables among PU or PEOU as following: self-efficacy-PEOU, subjective norm-PU, self-efficacy-PU, interaction-PU, enjoyment-PEOU, anxiety-PEOU, enjoyment-PU, compatibility-PU, subjective norm-PEOU and interaction-PEOU

Table 8 Continued

Author	**Model**	**Constructs**	**Purpose**	**Findings**
Seta et al. (2018)	DeLone & McLean IS model	Technical system quality, service quality, content and information quality, use, user perceived satisfaction, and individual impact	The goal of this study was to develop an integrated model to measure the success of e-learning in Indonesia	Individual performance is impacted by the use and satisfaction of e-learning systems. Furthermore, the researchers found that educational system quality and technical quality were the most significant factors influencing e-learning system user satisfaction, whereas the use of e-learning systems is influenced by the quality of the information and content, as well as the perception of the user of the system.
Al-Rahmi et al. (2019)	TAM and Diffusion Innovation Theory (DIT)	Relative advantages, observability, trialability, perceived compatibility, complexity, and perceived enjoyment	The paper proposed an extended technology acceptance model (TAM) that has been tested and examined with both innovation diffusion theory (IDT) and integrating TAM	The six variables shew an insignificant impact on the PEOU. While it had a strong influence on PU. Therefore, the acceptance of the e-learning system used to improve the students' learning performance, which can help decision makers in higher education.
Ansong-Gyimah (2020)	TAM	PU, PEOS, Attitude, Continuous ITU	The study examined the predictors of continuous intention to use Google Classroom	The attitude towards Use e-learning systems mediated the impact of PU and PEOU on Continuous Intention to Use Google Classroom.

Table 8 Continued

Author	**Model**	**Constructs**	**Purpose**	**Findings**
Almaiah & Alyoussef (2019)	The Unified Theory of Acceptance and Use of Technology (e-UTAUT) model	The factors of course design, course content support, course assessment, instructor characteristic, social influence, and actual use	The research utilized UTAUT to study the acceptance of e-learning systems in the Saudi Arabian context.	The utilization of e-learning systems was notably influenced by course design, course content support, course assessment, and instructor characteristics. However, the impact of social influence on actual usage was found to be statistically insignificant. Conversely, course design, course content support, and course assessment factors exhibited a positive effect on the perceived performance expectancy of e-learning systems.
Seliana et al. (2020)	DeLone & McLean IS model	Information, system, and service quality. In addition, use, user’s satisfaction, and perceived benefits.	Key objectives of this study were to evaluate lecturers' perceptions of e-learning implementation, assess its success, and identify the factors that influence e-learning implementation in the ABC Faculty at XYZ University.	Lecturers' perceptions of the implementation of e-learning were very positive. Effectiveness was found to be the most influential aspect of its implementation, followed by the semantic and technical aspects. Factors that influenced the successful implementation of e-learning included information quality, use, and user satisfaction with the e-learning systems implemented.

Table 8 Continued

Author	Model	Constructs	Purpose	Findings
Abbad (2021)	The unified theory of acceptance and use of technology (UTAUT)	Performance expectancy, effort expectancy, social influence, and facilitating conditions.	Model was utilized to analyze students' intentions to use and their actual usage of Moodle, an e-learning system at Hashemite University, a public university in Jordan.	Performance expectancy and effort expectancy influenced behavioral intentions to use Moodle, but not social influence. Additionally, students' use of Moodle was directly influenced by their behavioral intentions and facilitating conditions.
Alam et al. (2021)	TAM, e-learning quality (ELQ) model, User Satisfaction (USM) Model, IS Model,	Learner's quality, instructor's quality, information's quality, system's quality, and institutional quality	The objective of the study was to propose a comprehensive framework for e-learning services, with the aim of ensuring the efficient delivery and utilization of such services. The proposed framework aimed to enhance sustainable learning and improve academic performance.	The most affecting variables toward success of e-learning systems were the use of e-learning system, followed by PU, system quality, institutional quality, and instructor quality.

Table 8 Continued

Author	**Model**	**Constructs**	**Purpose**	**Findings**
Alotaibi & Alshahrani (2022)	DeLone & McLean IS model	Instructor quality, learner quality, perceived usefulness, information quality, system quality, and service quality	Students' responses were analyzed to identify the factors contributing to the success of the e-learning platform at Shaqra University.	According to the results, the model fits the Saudi context reasonably well. Instructor quality, learner quality, and perceived usefulness all positively impacted the e-learning platform. In contrast, information quality, system quality, and service quality did not affect the use of the e-learning platform.
Rokhman et al. (2022)	DeLone & McLean IS model	Student’s capability, teacher’s capability, and social influence, user’s satisfaction, System, information, and service quality	A revised version of the D&M ISS Model was used in this study to measure e-learning's effectiveness.	In this study, user satisfaction was determined by improving the quality of the system, the quality of information, the capability of teachers, the capability of students, and the social impact of the system. Additionally, students' satisfaction was found to be positively related to net academic benefit.
Al-Fraihat et al. (2020)	Comprehensive model based on DeLone & McLean IS model, TAM, e-learning satisfaction models and e-learning quality models.	Seven factors of quality: system, information, service, educational, support, learner, and instructor. In addition, PU, perceived satisfaction, and use.	The study successfully constructed a comprehensive model that offers a holistic perspective and identifies various levels of success in relation to a wide range of determinants.	The determinants for the e-learning systems’ benefits were the PU, perceived satisfaction, and use.

Table 9

Studies Utilized TAM to Examine e-Learning Platforms From Cybersecurity Perspective

Author	Constructs	Purpose	Findings
Tick (2018)	IT security awareness, social factors, smart tools, digital learning, traditional learning, and computer and internet literacy	The study was conducted to investigate the relationship between IT security awareness and social factors, digital learning, and smart phone usage. Moreover, the research examined the nature of computer and internet literacy, as well as IT security awareness among members of the early Z generation.	It was found that the greater IT security awareness of students, the more they will benefit from digital learning (DL) and use smart tools (ST). Furthermore, students who prefer DL and use ST are aware of the need for IT security. E-learning systems are implemented in an IT security conscious manner, as evidenced by the significant correlation between IT security awareness and e-learning system use. In addition, DL and ST have a positive correlation, which supports the view that digital natives - even those from the early Z generation - have a higher understanding of technology.
Alammary et al. (2021)	Attitudes, self-efficacy, effort expectancy, reliability, facilitating conditions, and cybersecurity awareness	The study examined the impact of the COVID-19 pandemic on the adoption of e-learning solutions and explored how this compelled experience would influence the long-term adoption of such solutions.	Behavioral intention to adopt e-learning is significantly affected by attitudes toward e-learning, self-efficacy, and perceived reliability. Moreover, COVID-19 positively influences e-learning adoption in the long run.

Table 9 Continued

Author	Constructs	Purpose	Findings
Malanga et al. (2022)	Quality (cybersecurity issues including reliability, assurance, responsiveness, and tangibility), social influence, facility conditions, effort expectancy, and habits.	This study has been recently conducted to examine students' acceptance of and intention to use Learning Management Systems (LMSs) for university education in Brazil utilizing the extended technology acceptance model, unified theory of acceptance and use of technology (UTAUT) and incorporating quality constructs adapted from the Service Quality Evaluation Model (ServQual).	It was found that facility conditions, habits, social influence, effort expectancy, and quality explained 80% of use intentions. With the exception of effort expectancy, which represents how students gain knowledge, productivity, and agility through the use of LMS, all constructs were significant and positive for LMS users.
Chai et al. (2022)	Internal factors (perceived usefulness and ease of use), external factors (perceived severity and perceived susceptibility), and intention to use.	As part of the COVID-19 outbreak, this study examined how external technical factors and internal personal factors influence telecommuting use intentions.	Users' favorable attitudes towards telecommuting are strongly influenced by perceived usefulness and perceived ease of use. As previously found in the TPB field, attitudes, normative influences, and perceived behavioral control all influence telecommuting adoption positively. Furthermore, perceived severity positively correlates with attitudes and normative influences. Although perceived susceptibility affects normative influence, it does not affect attitudes significantly.
Khalaf et al. (2022)	Online examination, course administration, assignment evaluation, feedback, student, and material management.	Blackboard was examined to suggest a learning management system accommodates the major capabilities of e-learning.	Technological innovations, e-learning service performance variables, trust variables, self-efficacy variables, and cultural influences were crucial determinants of e-learning systems.

Summary of Chapter Two

This study has focused on explaining concepts, terms, and concerns in cybersecurity, privacy, and integrity issues in the e-learning environment. The development of information and communication technology and the high reliance on the internet to accomplish most of the assigned work, tasks, or even homework at different levels make it difficult to control students' behavior in the digital world of e-Assessment. Cybercrimes are not only occurring in the sectors of economy, finance, or accounting, but also, they have been expanded to intervene in the educational sector. COVID-19 pandemic forced schools, universities, and different types of organizations around the world to transform their learning from in-person mode to virtual. Based on this, it is important to take many factors in consideration to ensure the progress of the educational process with achieving the goals for both faculty and students.

This section of this study shines the light on key dimensions which are vocal and critical points to sustain e-learning platforms and trust e-assessment that is provided in terms of service which tends to improve academic performance. Cybersecurity, privacy, awareness in cybersecurity, computer self-efficacy (CSE), and academic integrity (AI) concerns in education are essential to trust any systems. Consequently, awareness dissemination is needed at any stage of building, developing, or adopting LMSs as mediums to reach the desired academic objectives.

Chapter Three: Methodology

Quantitative Research Design

This present study utilized the quantitative research design, or deductive approach, to conduct this study. Quantitative research is conducted by using numerical data for the purpose of confirming or testing existing theory or hypotheses by measuring variables of interest (Leedy & Ormrod, 2019). This type of research ends with generalizable findings and results. According to the quantitative research design, the numerical data can be gathered by multiple instruments such as questionnaires with closed-ended questions that was utilized in this research work. Instruments can be deployed in quantitative research to collect data like observations which can be recorded in numbers and experiments (Williams, 2007). In this research, the collected data were analyzed statistically, and presented in tables and graphs. Various types of statistical analysis were utilized in quantitative research. For example, frequency analysis and descriptive analysis are commonly used to draw inferences about the selected sample and analyze the adopted scales/variables in the study. Descriptive analysis contains both the central tendency and dispersion measures which enable researchers to understand their data correctly, since it was important to check normality of data among all employed variables to be able to precisely determine which analysis to be performed. For instance, if dependent variable is highly skewed or ordinal level of measurement, in this case non-parametric analysis like Mann Whitney or Kruskal analysis is the appropriate ones in conducting the study.

The methodology section of the quantitative research design explained which theory has been adopted to serve the goals of the study. The variables in the proposed conceptual model in this research were measured by preparing a set of questions or statements which represent these variables. Each item in the questionnaire was rated numerically by using a 5-point Likert scale as an example. In this section, priori hypotheses have been developed which represent the expected relationship between different combinations of variables. Quantitative research requires adequate size of participants to avoid bias problems. According to the probability theorem, it is recommended to have large sample size (Martínez-Mesa et al., 2014). In addition, there should be a demonstration of the tool or instrument that has been used for the data collection process.

Human Subjects' Approval

To conduct human subject research, permission was requested from the university's institutional review board (IRB) administrators prior to collecting relevant information for the study. In accordance with the IRB, a formal application was filed, and the process was completed before the study began. The students' supervisors ensure meticulous adherence to the IRB process, protecting the privacy of research subjects.

IRB and consent issues such as the goal of study and participant rights to withdraw or cancel their participation at any time must be clarified and reported in this section too. The variables used in the study are supposed to be defined and linked to the literature review section. Finally, the researcher described the technique of testing hypotheses and determined the level of significance (alpha) which would be used to accept or reject null hypothesis (H0), usually alpha is equivalent to 0.05. Null hypothesis was rejected when alpha is equal to or less than 0.05.

Study Type

This research work was a cross sectional study that will include all undergraduate and graduate students at Eastern Michigan University (EMU). Cross-sectional study is a type of observational study through which the investigator can do measurements on outcomes and exposures of participants at the same time. Cross-sectional design can assist in conducting population-based survey studies. Participants in cross-sectional studies can be selected based on the investigator’s criteria. This type of study can be conducted quickly and inexpensively with a large audience of participants (Setia, 2016). Cross-sectional studies enable researchers to estimate the prevalence of outcomes of interest because of the sample selection from the main suggested population. Also, any potential risk factors or outcomes can be easily assessed. Finally, deploying this type of study allows less possibility of loss to follow up (Levin, 2006).

Study Population and Sample

The population of this study will be all undergraduate and graduate at EMU. Whereas the sample had 582 undergraduates and graduates from EMU. Convenience sampling technique was utilized in this study. A convenience sample is a non-probability sampling method by which researchers collect market research data from respondents who can be accessed conveniently. It is the most frequently used sampling technique because it is quick, simple, and inexpensive (Stratton, 2021). It is often easy for members to participate in the sample (Etikan et al., 2016). In convenience sampling, no additional inputs are required for primary research. This sample is open to anyone who meets the criteria (Emerson, 2015). Consequently, incorporating elements into this sample becomes incredibly straightforward. In order to participate in the sample, all components of the population must be within easy reach of the researcher.

Eastern Michigan University (EMU)

A public research university located in Ypsilanti, Michigan, EMU offers a variety of academic programs. EMU is one of Michigan's most diverse public universities, focusing on equity and inclusion as part of its core mission. EMU is the second-oldest public university in Michigan, having been founded in 1849. Currently, more than 15,000 students are studying for undergraduate, graduate, specialist, doctoral, and certificate degrees. The university offers more than 300 majors, minors, and concentrations across its Colleges of Arts and Sciences, Business, Education, Engineering and Technology, Health and Human Services, and Graduate School. A ranking for EMU was published in 2022 by U.S. News and World Report in the category of social mobility. This ranking reinforces Eastern's core value of being an institution where opportunities are available to all (EMU, 2022). The university offers classes in-person, hybrid, and full online (synchronous and asynchronous) delivery modes using e-learning platforms. Canvas is the learning management system (LMS) that is adopted at EMU.

Study Methods and Data Collection Process

The researcher has reviewed previous relevant literature to determine the variables that have been studied, so the researcher can support the proposed variables in the developed framework for this study. The proposed variables have been included in the developed questionnaire that will be used in the survey in this research. Qualtrics survey was deployed for building the proposed survey for collecting data. This online, close-ended questionnaire was distributed to the selected sample, which was expected to have the survey returned from at least 380 of undergraduate and graduate students at EMU (according to the sample size calculation based on the population size), using students' university email address. Appendix A shows a complete version of the proposed questionnaire designed for this study. The researcher asked for the IRB approval, then the Human Subject Review office was responsible to distribute the link of the online survey to 6,800 undergraduate and graduate students at EMU.

Data were analyzed using SPSS 28 software. Descriptive statistics, inferential statistics, correlations, and regression analysis have been conducted. Charts and diagrams were embedded in the study to visualize the data and present the findings**.** Finally, the study tested the formulated hypothesis (priori hypotheses) using SPSS, with an alpha value of 0.05 and a significance level of 0.95. Testing hypotheses helped in accepting or rejecting the null hypotheses (H0) based on the common probability rule that stated H0 is rejected when the p-value is equal or less than alpha (0.05) which indicates accepting the alternative hypotheses (H_a).

Literature Searching and Selection Procedure

This study was based on a systematic review of current research works in the field of cybersecurity, privacy, and awareness, CSE, and AI issues in online learning environments to build its proposed framework. Specifically, the study summarizes the current state of knowledge in the areas of cybersecurity, awareness, privacy, computer self-efficacy (CSE), and academic integrity (AI) concerns in e-learning platforms. For that purpose, various articles and theories regarding these aforementioned concepts were analyzed and synthesized. The literature review included most recent and relevant studies ranging from 2016 to 2023. The research articles from the current literature were included based on the following criteria: (a) Peer-reviewed publication in journal or conference proceedings, (b) written in English, (c) empirical data and studies published between 2016 to 2023. However, research articles on classic theoretical models published before 2016 were included too, (d) articles focusing on issues relevant to the topic of this study.

The deployed procedures for literature survey can be summarized as follows: summarize prior research, assess contributions of prior research, summarize, and illustrate the basic findings of prior research observed in research streams. Finally, the utilized articles in building the introduction and literature review sections were downloaded by using keywords for the search process such as cybersecurity perspectives in e-learning, cybersecurity and e-learning, privacy issues in e-learning, awareness of cybersecurity in e-learning platforms, training in cybersecurity in learning management systems (LMSs), electronic assessment (e-assessment) in e-learning, academic integrity in online learning, academic misconduct in digital education, e-Assessment and cybersecurity, privacy risks in LMSs, and computer self-efficacy. Below, the most relevant articles were also organized and categorized in a table summarizing the concept of e-assessment. See Figure 8, which demonstrates the total number of research articles which mainly consists of journals and conferences papers that are utilized to build this dissertation work project. The articles range from classical studies (that are published before 2016) to 2023. The chart shows that 75% of the used articles are journals, while the remaining 25% of the pie chart consists of conference papers and others like handbooks, book chapters, and published dissertations. See the pie chart in Figure 9.

SPSS Software for Data Analysis

SPSS is a Statistical Package for the Social Sciences (Sun, 2019) that is utilized to manipulate, analyze, visualize, and present data in expressible formats using charts, diagrams, or tables. SPSS package is widely used in the social and behavioral sciences. There are several versions of SPSS. The original version program is known as SPSS Base, and several add-on modules have extended the range of data entry and statistical or reporting capabilities (Devi et al., 2013). This research got benefitted from the capabilities and features that SPSS 28 provides, such as descriptive statistics, frequencies, correlations between scales, and regression analysis, which will help the study with building the model with the proposed variables and testing the developed hypotheses. SPSS Modeler consists of a set of data mining tools that allow users to quickly develop predictive models using business expertise and deploy them into business operations to improve decision making (Devi et al., 2013).

Timeline

- Dissertation work Defense was expected to be conducted at the end of this Fall semester between 12th and 14th of December 2022.
- Human Subjects Consent Development was conducted in the beginning of January in the first week of the Winter term 2023.
- Human Subjects and Organizational Approvals were expected to be achieved in the third or the fourth week of the next semester (the end of January 2023).
- Survey Administration took four to six weeks (the end of March 2023).
- Data Analysis, Reporting, and dissertation development took a month (the end of May 2023). Dissertation Committee Review would have at least two need two weeks. Dissertation Defense was scheduled on June 13, 2023.

Statistics of Literature Reviewed

Figure 8 and Figure 9 below show the extensive literature review to develop proposed conceptual model in this research dissertation work.

Figure 8

The Frequency of Research Articles That Are Utilized in This Dissertation Work

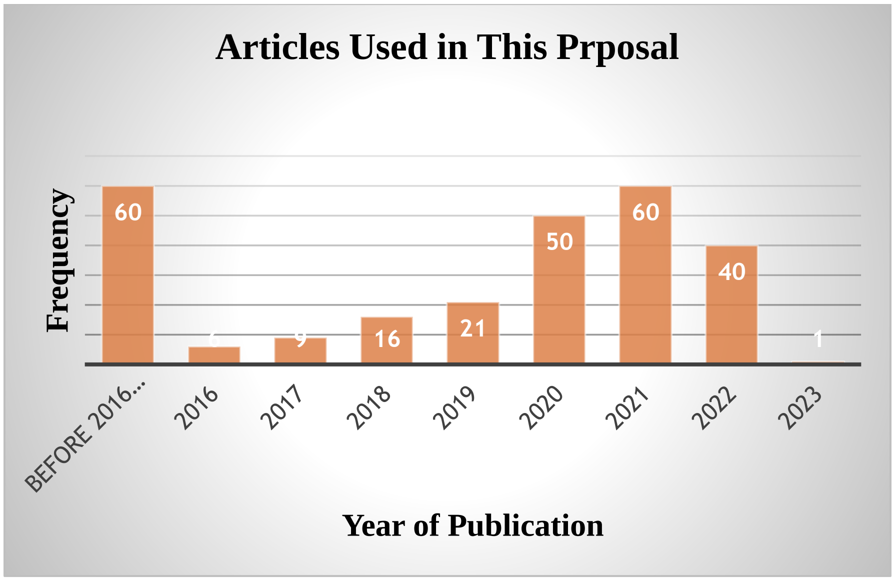
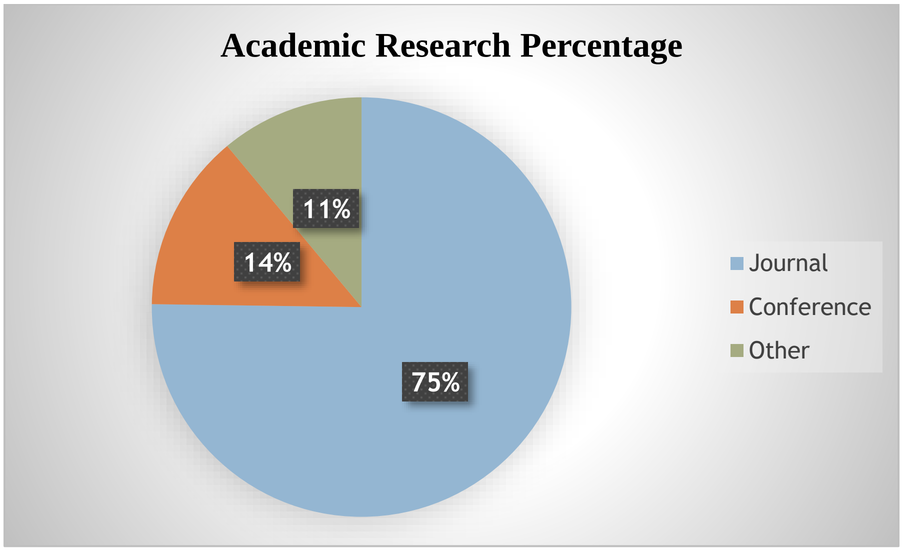


Figure 9

The Percentage of Each Research Work That Were Included in This Dissertation Work



Variables

Independent Variables (IVs)

This study includes demographic variables as they are illustrated in Table10. They are gender, ethnicity, discipline, and level of education of the selected sample. The level of measurement for the demographics is categorical levels. For instance, the proposed demographics variables for this study are categorical including nominal and ordinal measurement levels. The level of education is ordinal variable that consists of two possible answers undergraduates, and graduates. While the other remaining demographics (gender, ethnicity, and subject/discipline) are nominal.

Independent variables have been proposed based on the researcher's findings from the literature review section. Cybersecurity perspectives, privacy concerns, cybersecurity awareness, AI concerns, and CSE concerns are considered the independent variables for the proposed framework in this research. Each of the proposed independent variables has been represented by a set of statements written in the form of close-ended questions. After collecting data, the individual items were combined to compute the new scaled variable using mean function. The individual items which form these constructs are at an ordinal level of measurement since each single statement will be rated by a 5-point Likert scale ranging from *extremely disagree* to *extremely agree.* See Table 10 below.

Dependent Variable (DV)

The outcome variable was students' intention to use e-learning platforms. This variable was computed from all individual items (ordinal) that were relevant to this scaled construct in the proposed framework. These items are in ordinal level of measurement, they were rated by a 5-point Likert scale. See Table 10 below.

Table 10

Demographics Used in This Research Work

Variable	Description
Gender	□ Man □ Woman □ Transgender/Trans woman □ Transgender/Trans man □ Genderqueer/Non-Binary □ Not Listed: - …………………. □ Prefer not to reply.
Ethnicity	□ Hispanic □ Asian □ Native-American □ Arab □ African American □ Caucasian □ Not Listed: - ………………….
Subject/Discipline	□Computer-Related Major □ Non-Computer Related Major
Level of Education	□ Undergraduate □ Graduate

Testing Strategies

Validity Testing

The proposed questionnaire was assessed by a focus group to obtain their feedback based on their experience in the field of research (Shdaifat, 2020; Shdaifat et al., 2020). They evaluated the face validity of questions by examining the level of accuracy and relevance of each item to its appropriate scale. Scales are supposed to measure what they are designed to measure (Ursachi et al., 2015).

Reliability Testing

The reliability of the proposed questionnaire was measured by calculating Cronbach's alpha coefficient value for the built scales. The optimum value for Cronbach's alpha coefficient value is 0.85 (Shdaifat, 2020; Shdaifat et al., 2020). In addition, exploratory factor analysis (EFA) has been conducted for the purpose of developing instruments, reducing data, and building theory for this study. After performing component factor analysis (CFA), items with loading factors > 0.3 would be retained (Nunnally & Bernstein, 1994). The Kaiser-Meyer-Olkin (KMO) measure was considered to check the sampling adequacy. KMO values closer to 1.0 are considered ideal while values less than 0.5 are unacceptable. Bartlett's Test of Sphericity helped to assess the significance of correlation matrix and determine which variables were unrelated and not ideal for factor analysis (Tabachnick et al., 2007). Before distributing the questionnaire, the researcher followed the parallel forms of reliability method to test the consistency among the questions in the instrument. This technique required preparing two versions of the instrument with different questions measuring the same constructs and administering them to the same group of participants at the same session. Table 11 below explains the analyses that were employed in this study to answer the basic research questions.

Table 11

Analytical Matrix of the Basic Research Questions of the Dissertation Work

#	Research Question	Independent Variable (IV)	Dependent Variable (DV)	Analysis	Justification/ Assumption
1-	To what extent cybersecurity perspectives affect the students' intention to use e-learning platforms with controlling the other variables?	Cybersecurity perspectives (scaled variable), Privacy concerns, cybersecurity awareness, academic integrity concerns, and computer self-efficacy	Intention to use e-learning platforms. (Scaled variable)	Multiple regression	IV = Cybersecurity perspectives (scaled) DV = Intention to use e-learning platforms (scaled). Assuming that both variables are normally distributed and linearly correlated with each other.
2-	To what extent students' privacy concerns affects their intention to use e-learning platforms with controlling the other variables?	Privacy concerns (scaled variable), cybersecurity perspectives, cybersecurity awareness, academic integrity concerns, and computer self-efficacy	Intention to use e-learning platforms. (Scaled variable)	Multiple regression	IV = privacy (scaled) DV = Intention to use e-learning platforms (scaled). Assuming that both variables are normally distributed and linearly correlated with each other.

Table 11 Continued

#	Research Questions	Independent Variable (IV)	Dependent Variable (DV)	Analysis	Justification/ Assumption
3-	To what extent cybersecurity awareness affects the students' intention to use e-learning platforms with controlling the other variables?	Cybersecurity awareness (scaled variable), cybersecurity perspectives, privacy concerns, academic integrity concerns, and computer self-efficacy	Intention to use e-learning platforms. (Scaled variable)	Multiple regression	IV = Cybersecurity Awareness (scaled). DV = Intention to use e-learning platforms (scaled). Assuming that both variables are normally distributed and linearly correlated with each other.
4-	To what extent academic integrity concerns affect the students' intention to use e-learning platforms with controlling the other variables?	Academic integrity (AI) concerns (scaled variable), cybersecurity perspectives, privacy concerns, cybersecurity awareness, academic integrity concerns, and computer self-efficacy	Intention to use e-learning platforms. (Scaled variable)	Multiple regression	IV = Academic integrity concerns (scaled). DV = Intention to use e-learning platforms (scaled). Assuming that both variables are normally distributed and linearly correlated with each other.

Table 11 continued

#	**Research Questions**	**Independent Variable (IV)**	**Dependent Variable (DV)**	**Analysis**	**Justification/ Assumption**
5-	To what extent students' computer self-efficacy affects their intention to use e-learning platforms with controlling the other variables?	Computer self-efficacy (CSE), cybersecurity perspectives, privacy concerns, cybersecurity awareness, academic integrity concerns, and computer self-efficacy	Intention to use e-learning platforms. (Scaled variable)	Multiple regression	IV = computer self-efficacy (scaled). DV = Intention to use e-learning platforms (scaled). Assuming that both variables are normally distributed and linearly correlated with each other.

This research work attempted to answer the following main question regarding the demographics' effect on the proposed variables in this study. See Table 12.

To What extent do the demographics affect the five proposed predictors?

a. *Do Cybersecurity perspectives differ by level of education?*

b. *Do the Privacy concerns differ by gender?*

c. *Does Cybersecurity Awareness differ by discipline?*

d. *Do Academic Integrity concerns differ by ethnicity?*

e. *Does the Computer Self-Efficacy differ by discipline?*

Table 12

Analytical Matrix (B)–Demographics Effect on the Proposed Predictors

#	Research Question	Independent Variable (IV)	Dependent Variable (DV)	Analysis	Justification/ Assumption
6-a	Do cybersecurity perspectives of students differ by level of education?	Level of education (2-***level Ordinal***	cybersecurity perspectives ***Scaled variable***	Independent samples t-test	Level of education = IV (Categorical ordinal with 2 groups) Cybersecurity = DV is scaled variable
6-b	Do privacy perceptions of students differ by Gender?	Gender **(7-level Nominal**)	Privacy perceptions. ***Scaled variable***	One-way ANOVA	Gender = IV (Categorical with more than 3 groups). Privacy = DV is scaled variable.
6-c	Does the awareness of cybersecurity concerns differ by the discipline?	Discipline (2-levels Nominal)	Cybersecurity Awareness scaled ***variable***	Independent samples t-test	Discipline = IV (nominal) Awareness = DV (scaled).
6-d	Do academic integrity concerns differ by ethnicity?	Ethnicity (Nominal-6 levels)	AI (scaled variable)	One-way ANOVA	Ethnicity =IV (categorical / nominal with more than 3 groups). AI=DV (scaled).
6-e	Does the computer self-efficacy differ by discipline?	Discipline (2-levels Nominal)	CSE (scaled variable)	Independent samples t-test	Discipline = IV (nominal) CSE = DV (scaled).

Data Analysis

Type of Analysis

The researcher has reviewed previous literature that discussed topics relevant to this research work and articulated the used variables that contributed to building the proposed framework. This study conducted multiple analyses to answer its proposed research questions (RQs). Descriptive statistics, independent sample t-test, one-way ANOVA, inferential statistics, Cronbach's alpha, and linear and multiple regression analysis will be conducted. Descriptive statistics will include central tendency and variability measures, such as mean, mode, median, range, variance, and standard deviation.

Assumptions of Each Analysis

Most quantitative research work start the analysis with Descriptive and inferential statistical analysis. In any study that includes categorical variables, the analysis of the categorical variables (nominal or ordinal) requires performing frequency analysis to observe the count or percentages among each category. While non-categorical data will utilize descriptive analysis to provide multiple tendency and dispersion measures, from the calculated statistics the researcher can draw an inference that helps to answer research questions. Comparison of means can help in providing answers to questions asking about the differences among groups by certain variable(s). The study has deployed independent samples t-test to test the differences between categorical (nominal/ordinal) independent variable that consists of only two groups, and a scaled (interval/ratio) dependent variable. Whereas the categorical independent variables which compose three or more groups will be included within one-way ANOVA with a scaled dependent variable. In the case of having two or more fixed factors (categorical independent variables) and one scaled dependent variable, it was supposed to prepare.

Finally, the regression analysis has less restricted assumptions, it assumes there is a true linear correlation between variables, observations are independent, errors are normally distributed, and there are equal covariances among groups. Regression analysis can be performed by using either categorical or non-categorical variables, but scaled ones are more preferrable.

Linear Regression. Linear regression analysis predicts the value of a variable based on its relationship to another variable. One or more independent variables are used to estimate the coefficients of the linear equation that best explain the dependent variable's value. Using linear regression, the difference between predicted and actual output values is minimized by fitting a straight line or surface.

Multiple Regression. Multiple regression analysis offers the optimal linear combination of independent variable scores that effectively elucidate the scores on the dependent variable. It generates a statistic known as multiple correlation (R), which represents the correlation between predicted scores on the dependent variable and the actual scores. A correlation value of 0.70 or higher indicates a strong and positive correlation, signifying that the model demonstrates a good fit and explains a substantial portion of the variation within the dependent variable.

Multiple regression analysis aids researchers in determining the direction and strength of the relationship between a specific predictor and the outcome variable, independent of other predictors. This is achieved by generating regression coefficients, which act as slopes that illustrate the association between the predictor variables (independent variables) and the outcome variable (dependent variable). Each coefficient represents the magnitude of change (beta or β) in the dependent variable. Thus, a one-unit increase or decrease in the specified predictor, while holding other predictors constant, will impact the dependent variable by the exact magnitude of the coefficient (β).

This dissertation work conducted the Multiple regression analysis because it was an appropriate method for data analysis since it provides comparable output statistics allowing the researcher the ability to compare the direction and magnitude of the different predictors used in this study.

Proposed Regression Model

For this study the expected regression equation is to be as the following:

Intention to Use e-Learning Platforms = β0 + β1* Cybersecurity Perspectives - β2 * Privacy concerns - β3 * Academic Integrity concerns + β4 * Cybersecurity Awareness + β5 * Computer Self-Efficacy+ εi

It was noticed from the regression model above that the dissertation work hypothesizes a positive correlation between (cybersecurity awareness and computer self-efficacy) with the dependent variable (intention to use e-learning platforms). On the other hand, there would be inverse relationships between (Cybersecurity, privacy, and academic integrity) with the intention to use e-learning platforms. It is important to clarify that β0 is the constant, while β is the size of effect or the change rate in which one unit change (increases or decreases) in any independent variable will lead to β change (increases or decrease) in the dependent variable.

Research Hypotheses of the Basic Research Questions

It was expected that both privacy and academic integrity (AI) concerns would be significant predictors of the intentions to use e-learning platforms. It was hypothesized that the three variables would affect the intention to use e-learning platforms negatively. On contrast, the other three variables, the cybersecurity perspectives, computer self-efficacy (CSE), and cybersecurity awareness would significantly affect the intention to use e-learning platforms in a positive way.

The researcher predicted that the increase in privacy and academic integrity (AI) concerns would lead to a decline in the students’ willingness to adopt e-learning platforms for education in future. In contrast, the researcher believed when there was an increase in students’ cybersecurity perspectives, capabilities and confidence level as well as the awareness of how to use the computer and internet technologies, the probability to adopt e-learning platforms goes up.

For the intention to use e-learning platforms variable, it was expected that students who are full time employees would prefer registering for asynchronous classes due to the amount of flexibility and convenience can be provided through this mode of instructions.

Research Hypotheses of the Mean Comparison Questions of Demographics

The study expects that privacy perceptions of students would differ by gender. It was believed that females would be more concerned regarding their privacy matter more than males. In addition, there would be significant differences among cybersecurity awareness and CSE by discipline because it was expected that students from technology related subjects (majors) would be more aware of the recent cybersecurity threats which may affect e-learning platforms more than other students from non-technology related background. Consequently, students who are aware of technological risks would be more confident of how to master these technologies.

On the other side, it was believed that cybersecurity perspectives would differ by the level of education (graduate or undergraduate) because graduate students are expected to be more careful regarding the value of the material and content which they submit over the leaning management system. For example, every submitted paper in any class may produce an initial idea for a big project for thesis or a dissertation. As a result, graduate students would be more concerned regarding cybersecurity issues rather than undergraduates.

Priori Hypotheses-Demographics

- Ha_1: There is a significant difference in the mean of students' cybersecurity perspectives by level of education.
- $H0_1$: *There is no significant difference in the mean of students' cybersecurity perspectives by level of education.*
- Ha_2: There is a significant difference in the mean of students' privacy concerns by gender.
- $H0_2$: *There is no significant difference in the mean of students' privacy concerns by gender.*
- Ha_3: There is a significant difference in the mean of students' cybersecurity awareness by discipline.
- $H0_3$: *There is no significant difference in the mean of students' cybersecurity awareness by discipline.*
- Ha_4: There is a significant difference in the mean of students' academic integrity concerns by ethnicity.
- $H0_4$: *There is no significant difference in the mean of students' academic integrity concerns by ethnicity.*
- Ha_5: There is a significant difference in the mean of students' computer self-efficacy by discipline.
- $H0_5$: *There is no significant difference in the mean of students' computer self-efficacy by discipline.*

Research Implication

This study plays an essential role in identifying the main strengths and weaknesses of e-learning platforms at the university level in general and learning management systems (LMSs) that are adopted in a certain university. The researcher has developed a questionnaire with close-ended questions which precisely explored the perceptions of students regarding the use of e-learning platforms from multiple vital dimensions such as security, privacy, and self-efficacy concerns. The participants' responses were rated by a 5-pint Likert scale as was mentioned earlier in the dissertation work. The weighted answers could spot the light on the most individual concerns in each used scale. Consequently, any observed gap between the students' perceptions and their expectations of how the typical e-learning platforms that are supposed to can be revealed. As a result, this study notified the responsible departments or parties at universities with students' needs, demands, preferences, and desires. The research work would act as feedback from students to enhance strengths and fix any possible deficiencies in the deployed e-learning platforms.

Summary of Chapter Three

This quantitative research work is a sectional study that aims to utilize TAM as a theoretical framework to examine the perceptions of students at EMU toward accepting the e-learning platforms according to the cybersecurity perspectives, cybersecurity awareness, privacy concerns, academic integrity (AI) concerns, and computer self-efficacy (CSE) factors. To achieve this purpose, the dissertation work plans to employ an online questionnaire with closed-ended questions that are rated by using 5-rate Likert scale which ranges from 1 (*extremely disagree*) to 5 (*extremely agree*).

Qualtrics survey was deployed for building the proposed survey for this study. Afterward, the link of prepared survey was distributed by Emich emails of students at EMU. The collected data were cleaned and analyzed using SPSS 28 tool. Descriptive and frequency analysis of demographics were conducted to provide a better understanding of the gathered data. In addition, multiple regression analysis was prepared to reveal the effect of certain variables on other variable (s). Finally, comparisons of mean analysis were needed to answer the questions of difference among variables.

Chapter Four: Data Analysis and Discussion

Data Pre-Processing

Data pre-processing refers to a set of best practices that ensure the quality and cleanliness of data before it is used for analysis. These practices are deployed critically to ensure the quality and reliability of the data being used, and this process cleans, transforms, and prepares data for analysis and modeling. Data pre-processing or cleansing has several important goals. Firstly, it aims to address missing or invalid values by identifying and removing them, which is crucial to prevent bias in the analysis or model outcomes. Secondly, it removes duplicate records from the dataset to avoid duplication of observations. Thirdly, it normalizes and scales the data, ensuring that all variables are standardized and have similar distributions. Finally, it handles outliers by detecting and either removing or transforming them, thus minimizing the impact of extreme values on the analysis or model (Smith et al., 2023). In summary, pre-processing of data can increase the accuracy and robustness of the final dataset for analysis by avoiding common pitfalls and errors.

Sample of Study

This study had 582 participants from EMU who were included in the sample. The majority of the participants were women, with 363 (62%) females 179 (31%) males, and 40 (7%) participants in “others” category. About 42.1% of the participants were graduate students, while the remaining 57.7% were undergraduates. Most of the participants were from non-computer-related programs, which accounted for 452 (78%) participants, while 129 (22%) participants were from computer-related programs. The sample also included participants from various ethnicities, with 403 (69%) Caucasians, 44 (7.6%) Arabs, 42 (7.2%) Asians, 44 (7.6%) African Americans, 23 (4%) Hispanics, and 26 (4.5%) participants who did not disclose their ethnicity.

The variable for gender was recoded to include multiple categories. A value of 0 denotes males, 1 denotes females, and 2 denotes a third category named as “others.” The “others” category was created due to small group sizes and includes the following gender sub-groups, genderqueer/non-binary, transgender/trans man, transgender/trans woman, and those who did not disclose their gender. Similarly, the variable for level of education was recoded, with a value of 0 indicating undergraduate students and a value of 1 indicating graduate students.

The variable for discipline was recoded to include two categories. A value of 0 denoted non-computer related majors, while 1 denoted computer-related majors. Ethnicity was also recoded, with Hispanic represented by 0, Asian by 1, African American by 2, Arab by 3, Caucasian by 4, and those who did not disclose their ethnicity represented by 5. Frequency analyses were conducted for every variable of the demographics including gender, level of education, discipline, and ethnicity (see Tables 13–17 and Figures 10–13).

Table 13

Descriptive Analysis of Demographics

N	Gender	Level of Education	Discipline	Ethnicity
Valid	582	581	581	582
Missing	0	1	1	0

Table 14

Gender Frequencies

Valid	Frequency	Percent	Valid Percent	Cumulative Percent
Males	179	30.8	30.8	30.8
Females	363	62.4	62.4	93.1
Others	40	6.9	6.9	100.0
Total	582	100.0	100.0	

Figure 10

Gender Frequency

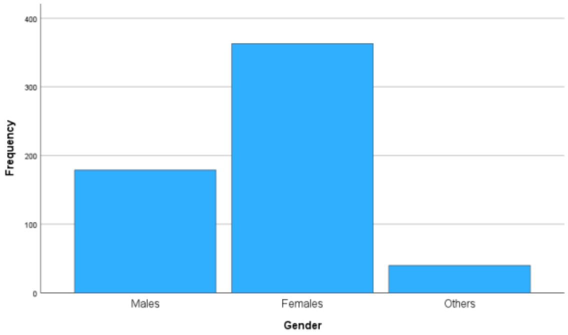


Table 15

Level of Education Frequencies

Valid	Frequency	Percent	Valid Percent	Cumulative Percent
Undergraduates	336	57.7	57.8	57.8
Graduates	245	42.1	42.2	100.0
Total	581	99.8	100.0	
Missing System	1	0.2		
Total	582	100.0		

Figure 11

Level of Education Frequency

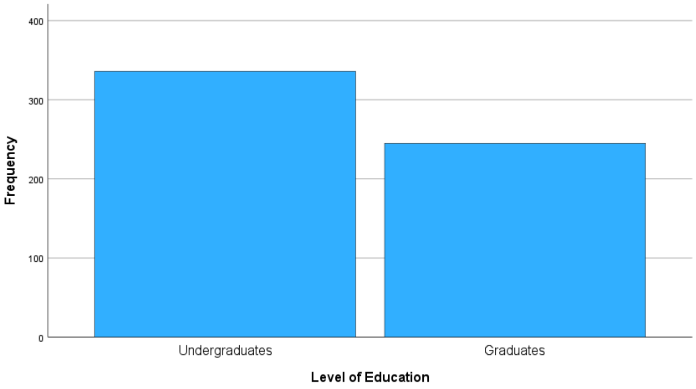


Table 16

Discipline Frequencies

Valid	Frequency	Percent	Valid Percent	Cumulative Percent
Non-Computer	452	77.7	77.8	77.8
Computer Related	129	22.2	22.2	100.0
Total	581	99.8	100.0	
Missing System	1	0.2		
Total	582	100.0		

Figure 12

Discipline Frequency

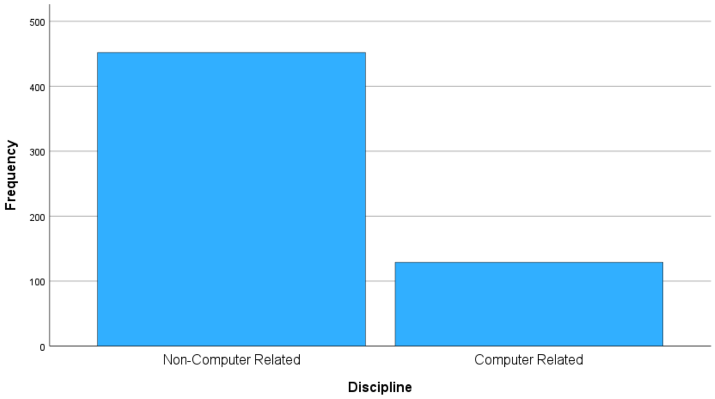


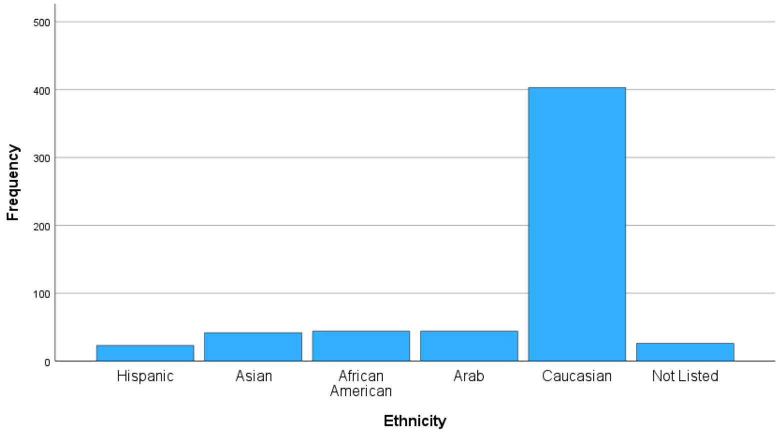
Table 17

Ethnicity Frequencies

Valid	Frequency	Percent	Valid Percent	Cumulative Percent
Hispanic	23	4.0	4.0	4.0
Asian	42	7.2	7.2	11.2
African American	44	7.6	7.6	18.7
Arab	44	7.6	7.6	26.3
Caucasian	403	69.2	69.2	95.5
Not Listed	26	4.5	4.5	100.0
Total	582	100.0		

Figure 13

Ethnicity Frequency



Reliability Analysis–Cronbach Alpha Values

Cronbach's alpha, also known as Cronbach’s coefficient alpha, is a measure of the reliability of a test or questionnaire. It is a coefficient that indicates the internal consistency or homogeneity of the items in a test. In other words, it assesses whether the items in the test are measuring the same underlying construct. Cronbach’s alpha is commonly used in psychology, education, and other subjects to evaluate the quality and reliability of tests and questionnaires. It is very important to ensure that items are reliable because unreliable measures can lead to invalid results, producing incorrect conclusions (George & Mallery, 2003).

The value of Cronbach's alpha ranges from 0 to 1, where higher values indicate higher reliability (George & Mallery, 2003). The alpha value is calculated based on the correlations between the items in the questionnaire. If all the items in the questionnaire measure the same underlying construct, the correlation between the items is high, and therefore, the alpha value is also high. A high Cronbach's alpha value (above 0.7) indicates that the items in the test are highly related to one another; therefore, the items are a reliable measure of the construct being assessed. On the other hand, if the items in the questionnaire measure different constructs, then the correlation between the items is low, and the alpha value is also low (George & Mallery, 2003). A low value (below 0.7) indicates that the items are not well-related and may not be a reliable measure of the construct.

Factor Confirmatory Analysis/Path Analysis

It is important to have a good understanding of statistics and causal inference when using path analysis, as well as a good understanding of the research problem and the variables being studied (Land, 1969). Factor analysis is a statistical technique used to identify underlying factors that explain the pattern of correlations among a set of observed variables. These factors can then be used to reduce the dimensionality of the data and to help understand the underlying structure of the variables (Yang, 2005).

To interpret the results of the factor analysis, this study examined the factor loadings for each item within each factor. Factor loadings represent the correlation between each variable and each factor. A high factor loading indicates that a variable is strongly associated with a particular factor (Taherdoost et al., 2022). The loading factor used for this analysis was 0.30. A variable with a loading factor of 0.30 or more indicated a strong association with only a particular factor or component.

In this case, the study examined the factor loadings for each variable on the three factors that were identified using factor analysis. It is possible that certain variables would have high loadings on one factor, indicating that they are strongly associated with that factor. This can help to interpret the underlying structure of the variables and identify common themes or constructs that the variables are measuring (Suhr, 2006). Additionally, it would be helpful to examine the communalities of each variable, which represent the proportion of variance in each variable that is explained by the factors. Communalities can help to identify variables that are not well explained by the factors and may need to be excluded from the analysis (Yong & Pearce, 2013). Overall, a factor analysis with three factors and a total variance explained of 61% suggests that there is some underlying structure to the variables that were analyzed, but additional factors or variables may need to be considered to fully explain the variation in the data.

Factor Analysis of the Independent Variables

The Cybersecurity Perspectives variable initially demonstrated a reliability of only 67.5% across all ten items. Two rounds of factor analysis were conducted, one including all ten items and another with the first eight items. These analyses revealed variances explained of 61% and 58.5%, respectively. The reliability test of the first four items yielded a high Cronbach's alpha value of 82.3%, while the last four items resulted in a value of 66.5%. Consequently, a reliability test was performed solely on the first eight items, which produced a more favorable Cronbach's alpha value of 78.7%. Therefore, the independent variable for Cybersecurity Perspectives was constructed using these eight items. As for items nine and ten, both exhibited a reliability of 85.3% and were determined to align better with the independent variable for privacy concerns based on factor analysis results. Hence, they were merged within the Privacy Concerns independent variable. Finally, the independent variable for Cybersecurity Awareness was tested for reliability through factor analysis, resulting in a single component with a Cronbach's alpha value of 87.3%.

Factor analysis was conducted for the independent variable of AI Concerns. This analysis resulted in two components for the seven items included in the AI Concerns variable, explaining a total variance of 72.4%. The first component consisted of the first four items, while the second component encompassed the last three items related to AI Concerns. To validate the new structure of the variables, a reliability analysis was performed. The first three items in the first component exhibited a Cronbach's alpha value of 77%, which was lower than the overall Cronbach's alpha value of 87.3% for all seven items. However, the remaining items in the second component demonstrated a reliability of 87.6%. Based on these results, a decision was made to include all seven items to represent the AI Concerns variable. The final independent variable was CSE, consisting of twelve items. Initially, a reliability test was performed on the first six items, resulting in a Cronbach's alpha value of 83.7%. The next six items yielded a slightly higher value of 84.4% of CSE variable. However, this study considered all 12 items as one component to create a unified independent variable. By doing so, Cronbach’s alpha value of 89.5% was obtained for the entire set of twelve items. Table 18 summarizes Cronbach's alpha values for all variables in this study. See Table 18 below.

Factor Analysis of Dependent Variable

Reliability testing was conducted for the dependent variable, Intention to Use (ITU), resulting in a Cronbach's alpha value of 52.4%. Subsequently, factor analysis was performed, which revealed two components that the six items were grouped into. To validate the new structure of the variable, a reliability analysis was conducted again. As a result, it was decided to remove Item #3, which stated, "I plan to take my classes offered in a hybrid format in the future." This decision was made because it was apparently a redundant question that essentially asked about the intention to register for online classes, rather than clearly reflecting the intention to use e-learning platforms.

Finally, Item #4 “I plan to take my classes offered in-person in the future” was reverse coded to serve the purpose of this scale and fit the direction of the remaining items in this scale. Reverse coding of survey items is a technique used to control response bias and ensure the validity of the results obtained from a survey. It involves reversing the coding of some of the survey items, such that responses that would normally be scored as "*agree*" are scored as "*disagree*," and vice versa. The purpose of reverse coding is to identify and control respondents who may be responding to survey items in a socially desirable or socially undesirable way, rather than responding truthfully based on their actual beliefs or experiences. Socially desirable responding occurs when respondents provide answers that they think are more acceptable or desirable, while socially undesirable responding occurs when respondents provide answers that they think are less acceptable or desirable (Mick, 1996). As a result of the reverse coding and subsequent reliability analysis, the scale achieved Cronbach's alpha value of 77.9%.

Table 18

Summary of Reliability-Test Values of All Variables

Variable	Cronbach' Alpha Value
Cybersecurity Perspectives	78.7%
Privacy Concerns	85.3%
Cybersecurity Awareness	87.3%
Academic Integrity Concerns	87.3%
Computer Self-Efficacy	89.5%
Intention to Use	77.9%

Computing Variables Process

After conducting a factor analysis, it is common to compute new variables or scores based on the factor loadings to use them for further analyses. These new variables are often called factor scores, factor-based scales, or composite scores. This study employed the mean function to compute the new scales because it provides a more accurate estimate of the participant's level of the underlying trait or ability, particularly when the items have different response scales or different levels of difficulty. Using the sum function may result in misleading estimates if the items have different levels of difficulty or if the response scales are not the same. Table 19 below demonstrates the final structure of each variable in this study.

Table 19

Final Structure of the Variables

Variable	**Total Items**	**items**
Cybersecurity Perspectives	8	1, 2, 3, 4, 5, 6, 7, and 8
Privacy Concerns	10	CST 9, CST 10, 1, 2, 3, 4, 5, 6, 7, and 8
Cybersecurity Awareness	6	1, 2, 3, 4, 5, and 6
Academic Integrity Concerns	7	1, 2, 3, 4, 5, 6, and 7
Computer Self-Efficacy	12	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12
Intention to Use	4	1, 2, Reverse-Coded 4, 5, and 6

Scales' Items

In this section, a comprehensive overview is presented of the items included in every scale within the questionnaire. The items have been meticulously designed to capture the essence of each construct under investigation. By including these items, this study aims to ensure a thorough exploration of the targeted dimensions and provide a holistic understanding of the phenomenon being studied. This section may serve as a valuable resource for researchers and readers alike, as it outlines the key elements that formed the foundation of this measurement instrument. See Tables 20-25 below.

Table 20

Cybersecurity Perspectives

#	Item / Question
CST1	e-learning platforms have a high security policy to protect students' sensitive information.
CST2	e-learning platforms are a secure place where I can share my sensitive information securely.
CST3	e-learning platforms are reliable and confidential.
CST4	e-learning platforms provide multi-factor authentication (e.g., phone number, password, PIN, SMS using smartphones, fingerprint), which makes me feel secure when logging into my account.
CST5	The grades obtained from e-exams or online exams in e-learning platforms are as valid and reliable as paper-based exams.
CST6	e-exams or online exams in e-learning platforms are fairer than paper-based exams.
CST7	Setting an automated timer for the whole e-exam and/or each question makes e-exams or online exams more secure than paper-based exams.
CST8	The technology used in online exams is sufficiently effective in dealing with cheating and plagiarism.

Table 21

Privacy Concerns

#	Item / Question
PV1	In the e-learning platforms, I feel uncomfortable providing my ideas or answers in the threaded discussion assignments.
PV2	In the e-learning platforms, my intellectual property (e.g., assignment work) is not protected.
PV3	In the e-learning platforms, I worry about the instructors recording (e.g., Zoom meetings) without my permission.
PV4	In the e-learning platforms, I feel uncomfortable during the proctored online exams because I am being watched and recorded.
PV5	The use of my personally identifiable information during the recorded, proctored online exams makes me feel I have less privacy.
PV6	Storing the recorded video of online exams and sharing them to the host server violates my privacy.
PV7	In the online group-based assignments and projects in e-learning platforms, there are less confidential and anonymous peer evaluations, which makes the evaluation process less fair in assessing peers' contributions.
PV8	In the e-learning platform, the instructors can detect my logs into the class and know the time I spend on the class, which makes me uncomfortable.
PV9	In the e-learning platforms, other students can detect and access my personally identifiable information, such as my email and profile, which makes me feel unsecure.
PV10	In the e-learning platform, the instructors can detect how often I log into the class which makes me feel uncomfortable.

Table 22

Cybersecurity Awareness

#	Item / Question
CSW1	I feel competent in using of computers.
CSW2	I have a good knowledge regarding computer hardware, software, and operating systems.
CSW3	I have a working knowledge of cyber-attacks which can occur over computer network systems.
CSW4	I have some knowledge about the concept of computer security measures, such as HTTPS, secure connection, SSH, and TSL.
CSW5	I have sufficient knowledge regarding the concept of “cyber-attacks”.
CSW6	I know the difference between “social engineering” and “phishing attacks”.

Table 23

Academic Integrity Concerns

#	Item / Question
AI1	In the E-learning platform, many students can share solved/completed assignments easily which makes me feel frustrated.
AI2	In the E-learning platform, many students can cheat easily, which makes me feel upset.
AI3	In the E-learning platform, many students can ask others to take the exam on behalf of them, which feels unfair.
AI4	In the E-learning platform, many students show carelessness in the online classes, which makes me feel less competent.
AI5	In the E-learning platform, many students either don’t comply with attendance or turn their cameras off, which makes online learning boring.
AI6	In the E-learning platform, many students show less respect to the course, which makes me feel uncommitted.
AI7	In the E-learning platform, many students show irresponsible behaviors in the course, such as playing with their cell phones, chatting, or playing games, which makes me feel unengaged in the course.

Table 24

Computer Self-Efficacy (CSE)

#	Item / Question
CSE1	To use e-learning platforms even if I had never used a system like it before, I would feel
CSE2	To use e-learning platforms if someone else helps me get started, I would feel
CSE3	To use e-learning platforms if I could call someone for help if I got stuck, I would feel
CSE4	To use e-learning platforms if I have just the built-in help facility for assistance, I would feel
CSE5	To use e-learning platforms if I have seen someone else using it before trying it myself, I would feel
CSE6	To use e-learning platforms if I have only the software manuals for reference, I would feel
CSE7	To use e-learning platforms if I have lot of time to complete my instructional job, I would feel
CSE8	To use e-learning platforms if no one is around to tell me what to do as I go, I would feel
CSE9	To use e-learning platforms if I had used similar systems before this one for instruction, I would feel
CSE10	To use e-learning platforms on my own, I would feel
CSE11	To download or install e-learning software/materials on my own, I would feel
CSE12	To navigate or search for document in any e-learning website, I would feel

Table 25

Intention to Use E-learning Platforms (ITU)

#	Item / Question
ITU1	I plan to take my classes offered online asynchronously in the future.
ITU2	I plan to take my classes offered online synchronously in the future.
ITU4- Reverse-Coded	I plan to take my classes offered in-person in the future.
ITU5	I will encourage others to take classes online.
ITU6	I prefer using the E-learning platforms over the traditional in-person, paper-based method.

Table 26

Computed Variables/Scales

	N	*Minimum*	*Maximum*	*Mean*	*Std. Deviation*	*Skewness*	*Kurtosis*
Cybersecurity Perspectives	*582*	*1.13*	*5.0*	*3.35*	*0.69*	*-0.26*	*0.005*
Privacy Concerns	*582*	*1.0*	*5.0*	*2.8*	*0.82*	*-0.08*	*-0.51*
Cybersecurity Awareness	*582*	*1.0*	*5.0*	*3.4*	*0.98*	*-0.16*	*-0.78*
Academic Integrity Concerns	*582*	*1.0*	*5.0*	*2.63*	*0.97*	*0.19*	*-0.64*
Computer Self-Efficacy	*582*	*1.0*	*5.0*	*3.54*	*0.67*	*-0.08*	*0.34*
Intention to Use	*582*	*1.0*	*5.0*	*3.14*	*1.01*	*-0.18*	*-0.75*
Valid N	*582*						

Missing Values in Dataset

The decision of when to remove missing values from a dataset depends on various factors, such as the percentage of missing values, the type of analysis planned to perform, the reason for the missing values, and the impact of the missing values on the accuracy of the analysis (Little & Rubin, 2019). If the percentage of missing values is small (e.g., less than 5%), it may be reasonable to retain the observations and fill the missing values with imputation methods or simply delete the missing values (Graham, 2009). This study decided to remove the empty rows that accounted for less than 0.05 of the total data to keep 582 instead of 590 cases.

Checking Normality

Checking the normality of a variable is an important step in many statistical analyses because it can affect the validity of the statistical tests that assume normality, such as t-tests and Analysis of Variance (ANOVA). This section summarizes two methods for checking normality. First, the visual inspection of the distribution is one of the easiest and most intuitive ways to check for normality. To do so, the researcher visually inspects the distribution of the variable using a histogram or a normal probability plot. A histogram can give a rough idea of the shape of the distribution, while a normal probability plot can provide a more precise assessment of normality by comparing the observed data with a theoretical normal distribution (Redfern, 2015).

In educational sciences, statistical techniques like t-tests, ANOVA, and Mann-Whitney U test are commonly employed for mean comparison. The specific technique chosen depends on the characteristics of the data sets, such as normality and equal variance. When the data is not normally distributed, the Mann-Whitney U test is utilized instead of the independent sample t-test (Orcan, 2020).

The second method for checking normality is to depend on the skewness and kurtosis values. Both skewness and kurtosis are measures of the shape of a probability distribution. They can be used to help determine if a dataset is approximately normally distributed, but they do not provide a definitive test for normality. Skewness measures the degree of asymmetry in the distribution. A skewness value of 0 indicates a perfectly symmetric distribution. Positive skewness indicates that the distribution has a longer tail on the positive side of the mean, while negative skewness indicates a longer tail on the negative side. However, it is important to note that a small amount of skewness does not necessarily mean that the distribution is non-normal. In practice, it is common to utilize skewness and kurtosis values as indicators for assessing normality. Some experts propose that these values can be as large as 2 in absolute terms. Conversely, standard errors of skewness and kurtosis have also been employed for normality tests. According to Kim (2013), if the skewness and kurtosis values are smaller than 1.96 times their respective standard errors, it indicates normality.

Kurtosis measures the degree of peakedness in the distribution. A kurtosis value of 0 indicates a normal distribution, while positive kurtosis indicates a more peaked distribution than normal and negative kurtosis indicates a flatter distribution than normal. However, it is also important to note that a small deviation from 0 does not necessarily indicate a non-normal distribution. In general, if a dataset has skewness and kurtosis values close to 0, it is more likely to be approximately normally distributed. However, it is still important to use additional methods to check for normality, such as normal probability plots or statistical tests like the Shapiro-Wilk test or the Kolmogorov-Smirnov test.

In this study, the assessment of normality relies on skewness values, taking into account the findings of Orcan's study (2020) as well as visual examination of histograms with normality curves. All variables in this study exhibit skewness values ranging from -0.5 to 0.5, indicating their proximity to zero. The highest skewness value observed is -0.26. These results provide evidence supporting the assumption that our data follows a normal distribution. As a result, parametric analyses are performed to address the research questions and test the proposed hypotheses. See table 26 above and histograms below.

Histograms with Normal Curve

Histograms with normal curve are an essential tool for assessing the normality of a data distribution. By visually comparing the shape of the histogram to the symmetrical bell-shaped curve of the normal distribution, researchers can gain insights into the underlying distribution of their data. This graphical representation provides a quick and intuitive way to identify departures from normality, such as skewness or excessive kurtosis. Checking the normality assumption is crucial for many statistical analyses, as several parametric tests rely on the assumption of normality. Recently, in a study by Smith et al. (2022), histograms with normal curve were employed to assess the normality of a sample distribution, ensuring the validity of subsequent inferential analysis. This emphasizes the continued relevance and practical utility of this technique in contemporary research.

Figure 14

Cybersecurity Perspectives Distribution

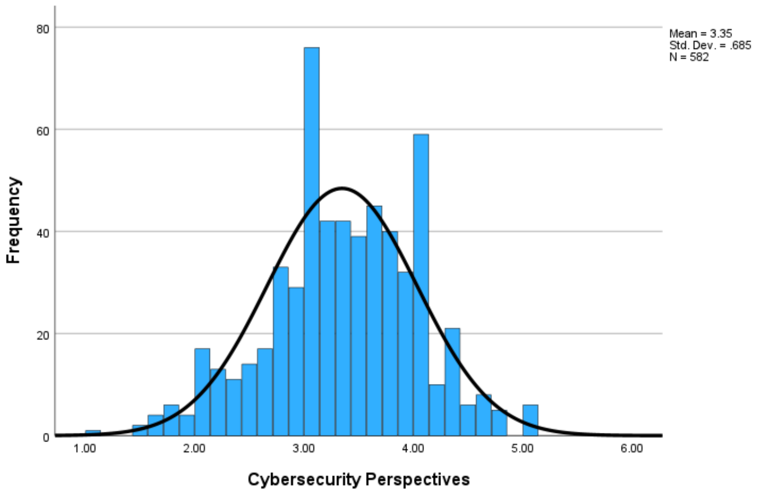


Figure 15

Privacy Concerns Distribution

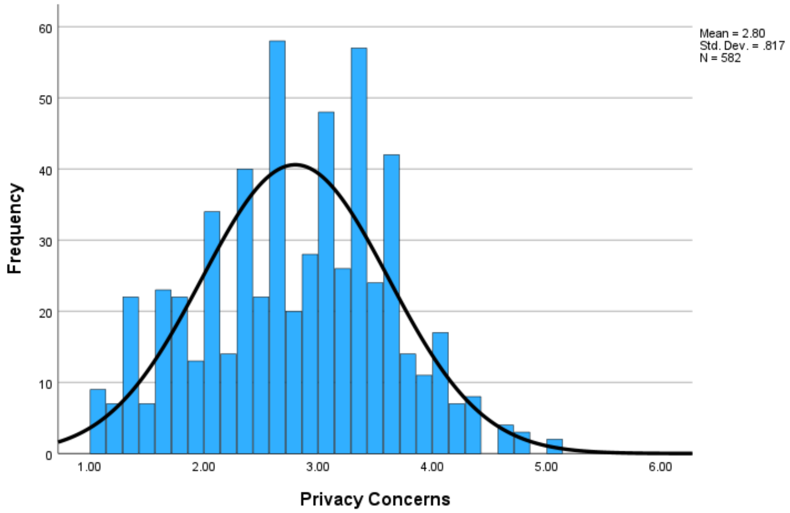


Figure 16

Cybersecurity Awareness Distribution

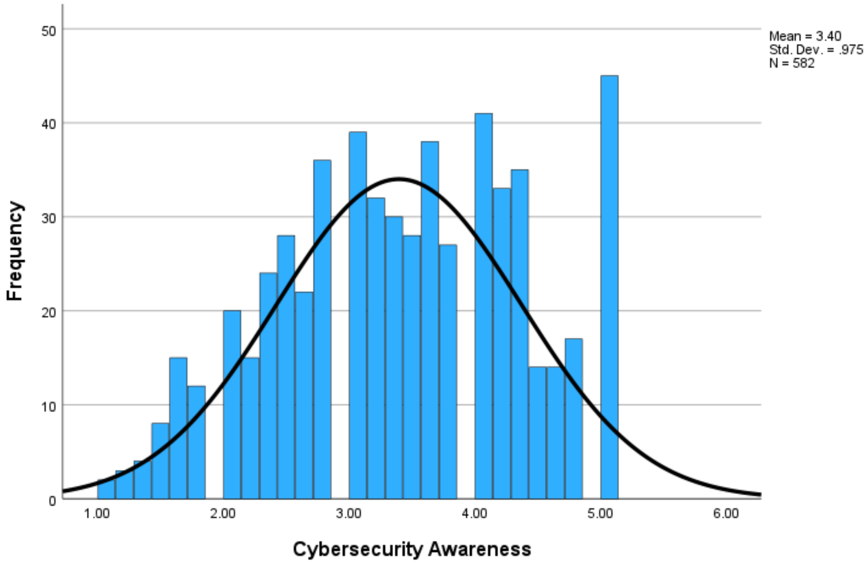


Figure 17

AI Concerns Distribution

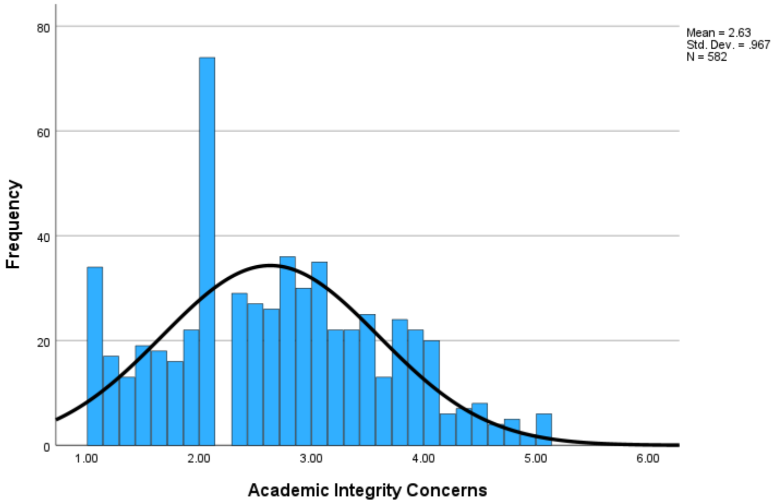


Figure 18

Computer Self-Efficacy (CSE)Distribution

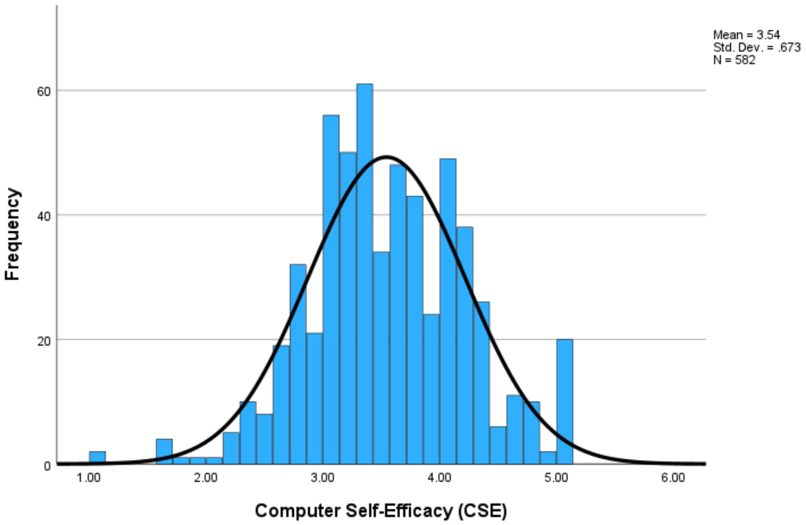
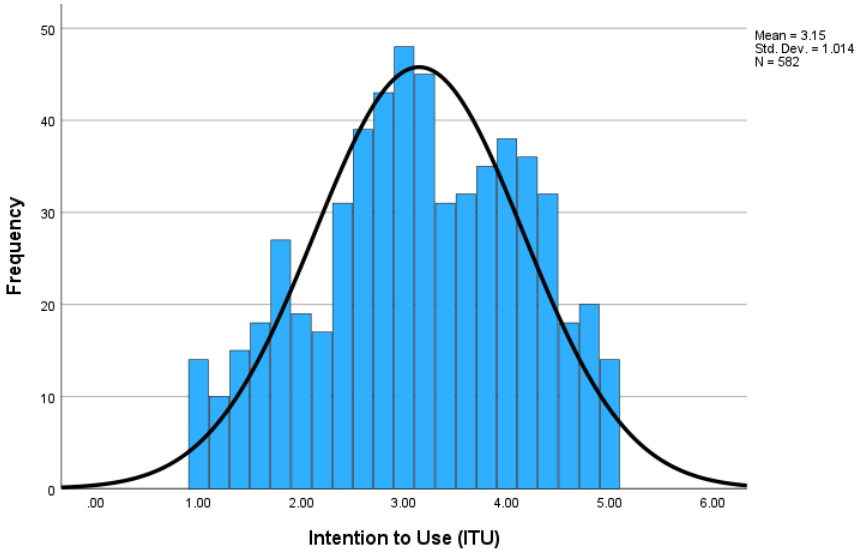


Figure 19

Intention to Use (ITU) Distribution



According to the histograms above (Figures 14-19), all of independent variables and the dependent variable for this study are normally distributed with considering of the skewness values between -0.5 and 0.5, indicating that the data in this study are normally distributed since

Skewness is a statistical measure that indicates the degree of asymmetry in a distribution of data. skewness values between -0.5 and 0.5 generally indicate that the distribution is approximately symmetrical. This means that the data is evenly distributed around the mean, with the same amount of data on both sides of the mean.

In other words, a skewness value between -0.5 and 0.5 indicates that the data is not significantly skewed to the left or the right, and the distribution is roughly bell-shaped. This is also known as a mesokurtic distribution, which means the data has a normal or Gaussian distribution. It is important to note that while a skewness value between -0.5 and 0.5 generally indicates a symmetrical distribution, other factors such as the sample size and the presence of outliers can also affect the skewness value. Therefore, it is always important to examine the distribution of the data visually and consider other statistical measures as well. As a result, the study proceeded to conduct parametric analysis including the comparison of means as well as the multiple regression.

Hypotheses Testing

Hypothesis testing is a statistical method used to make inferences or draw conclusions about a population based on a sample of data. It involves formulating two competing hypotheses, the null hypothesis (H_0) and the alternative hypothesis (H_a), and then collecting and analyzing data to determine which hypothesis is more likely. The null hypothesis typically represents the status quo or the absence of an effect, while the alternative hypothesis suggests that there is a specific effect or relationship between variables. The goal of hypothesis testing is to evaluate the evidence provided by the data and decide whether to reject or fail to reject the null hypothesis in favor of the alternative hypothesis (Mertler & Vannatta, 2016).

Hypothesis testing involves several steps. First, the null hypothesis, which assumes no significant difference or relationship, is formulated alongside the alternative hypothesis, which suggests a significant difference or relationship (Shaffer, 1995). A significance level, denoted as α, is then chosen to determine the threshold for rejecting the null hypothesis. Data is collected through experiments or sampling and is analyzed using statistical techniques to calculate the test statistic, which measures the deviation from the null hypothesis. The critical region is determined based on the significance level and the chosen statistical test, representing the range of values that would lead to rejecting the null hypothesis. A decision is made by comparing the test statistic to the critical region. If the test statistic falls within the critical region, the null hypothesis is rejected in favor of the alternative hypothesis, indicating evidence for a significant effect or relationship. Conclusions are then drawn about the population under study based on this decision.

Finally, hypothesis testing is a fundamental tool in statistical analysis and is used in various fields to make informed decisions and draw conclusions based on data (Page & Satake, 2017). It helps researchers and analysts evaluate theories, investigate research questions, and make evidence-based decisions. In this study, Pearson correlational analysis was conducted to examine the support or rejection of the hypotheses. Pearson correlational analysis is a statistical technique used to measure the strength and direction of the relationship between two variables (Prematunga, 2012). By applying this analysis, the researchers aimed to assess the degree of association between the variables under investigation and determine whether the observed data aligns with the proposed hypotheses. This approach allows for a comprehensive evaluation of the relationships and provides insights into the validity and significance of the hypotheses in question.

The Pearson correlation matrix displayed in Table 27 reveals significant associations between cybersecurity perspectives and the dependent variable, ITU, indicating a moderately positive relationship (Pearson = 0.35) with a high level of significance (*p* < .001). Conversely, privacy concerns exhibit an insignificant correlation (*p* = .15) with ITU, displaying a low negative relationship (Pearson = -0.06). Regarding the cybersecurity awareness variable, a low positive correlation (Pearson = 0.26) with ITU is observed, which is highly significant (*p* < .001). On the other hand, AI concerns display a significant and low negative correlation (Pearson = -0.28) with ITU, emphasizing its impact on the dependent variable. Lastly, CSE demonstrates a significant and low positive correlation (Pearson = 0.33) with ITU, underscoring its association with the dependent variable (*p* < .001). Table 28 shows the interpretation of every coefficient range which demonstrates the strength of relationship (Cohen, 1988). Finally, Table 29 summarizes the hypotheses results and the justification for each hypothesis where all of hypotheses were supported except H_{a2}.

Table 27

Correlation Matrix of the Independent and Dependent Variables

	Cybersecurity Perspectives	Privacy Concerns	Cybersecurity Awareness	Academic Integrity Concerns	Computer Self-Efficacy	Intention to Use
Cybersecurity Perspectives		-.215**	.155**	-.153**	.290**	. 349**
Sig. (2-tailed)		<.001	<.001	<.001	<.001	<.001
Privacy Concerns		1	.045	.234**	-.126**	-.059
Sig. (2-tailed)			.279	<.001	.002	.152
Cybersecurity Awareness			1	-.095*	.492**	.264**
Sig. (2-tailed)				.021	<.001	<.001
Academic Integrity Concerns				1	-.199**	-.280**
Sig. (2-tailed)					<.001	<.001
Computer Self-Efficacy					1	.325**
Sig. (2-tailed)						<.001
Intention to Use						1

Table 28

Correlation Coefficients Interpretation

Coefficient Range	**Strength of Relationship**
0.00 - 0.20	Very Low
0.20 - 0.40	Low
0.40 - 0.60	Moderate
0.60 - 0.80	High Moderate
0.80 - 1.00	Very High

Table 29

Basic Hypotheses Testing Result

#	Alternative Hypotheses	Decision	Justification
H_{a1}	Students' cybersecurity perspectives will have significant positive correlation with their intention to use e-learning platforms.	*Supported*	Pearson value shows a significant (*p-value* < 0.001) positive correlation (r = 0.35) between cybersecurity perspectives and the intention to use e-learning platforms.
H_{a2}	Students' privacy concerns will have significant negative correlation with their intention to use e-learning platforms.	*Rejected*	Pearson value shows an ***insignificant*** (*p-value* = 0.15 > 0.05) weak negative correlation (r = - 0.06) between privacy concerns and the intention to use e-learning platforms.
H_{a3}	Cybersecurity awareness will have significant positive correlation with students' intention to adopt e-learning platforms.	*Supported*	Pearson value shows a significant (*p-value* < 0.001) positive correlation (r = 0.264) between cybersecurity awareness and the intention to use e-learning platforms.
H_{a4}	AI concerns will have significant negative correlation with students' intention to adopt e-learning platforms.	*Supported*	Pearson value shows significant (*p-value* < 0.001) negative correlation (r = - 0.28) between AI concerns and the intention to use e-learning platforms.
H_{a5}	CSE will have significant positive correlation with students' intention to adopt e-learning platforms.	*Supported*	Pearson value shows a significant (*p-value* < 0.001) positive correlation (r = 0.33) between CSE and the intention to use e-learning platforms.

Means Comparisons Analyses

The Independent Samples T-Test

The independent samples t-test is a statistical method used to compare the means of two independent groups (Gerald, 2018). It is used to determine whether the mean difference between two groups is statistically significant or if it occurred by chance. In an independent samples t-test, data from two groups are collected, and the mean and standard deviation of each group are calculated. The t-test then calculates a t-value, which represents the difference between the means of the two groups, relative to the variability of the data within each group (Livingston, 2004).

In an independent samples t-test, the null hypothesis posits that there is no significant difference between the means of the two groups. If the calculated t-value exceeds a certain threshold, the null hypothesis is rejected, indicating a significant difference between the means of the two groups. The independent samples t-test assumes that the data follow a normal distribution and that the variances of the two groups are roughly equal (Lumley et al., 2002). If these assumptions are not met, alternative statistical methods may be employed to compare the means of the two groups (Nachar, 2008).

Mann Whitney U

Non-parametric analysis is a statistical approach that does not rely on any assumptions regarding the underlying distribution of the data being analyzed. The Mann Whitney U test, also referred to as the Mann-Whitney-Wilcoxon test or Wilcoxon rank-sum test, is a non-parametric test employed to compare two independent groups of data. The Mann Whitney U test is commonly used in research studies to compare variables in different groups, such as comparing the effectiveness of two different treatments on a particular health condition. It is also used in quality control to compare the performance of two different manufacturing processes (Nachar, 2008). The Mann Whitney U test is utilized when the data fail to meet the assumptions necessary for parametric tests, such as the t-test, which assumes normal distribution and equal variances (Nachar, 2008). In the Mann Whitney U test, the data from both groups are ranked, and the sums of the ranks between the two groups are compared to determine if a significant difference exists in the distributions.

The null hypothesis of the Mann Whitney U test is that there is no difference between the two groups being compared. The alternative hypothesis is that there is a significant difference between the two groups. If the calculated U value from the test is less than the critical value at the chosen significance level, then the null hypothesis is rejected, and it is concluded that there is a significant difference between the two groups (Nachar, 2008).

This study utilized the independent sample t-test to compare the means of two samples in order to examine the disparity in students' cybersecurity perspectives based on their level of education. This statistical test enabled the study to determine whether there is a significant difference in cybersecurity perspectives among students with varying educational levels (undergraduates and graduates). Furthermore, the Mann-Whitney U test was employed, which focuses on individual items within the cybersecurity perspectives independent variable. This particular test assisted the study in exploring the variations in students' perspectives on specific aspects of cybersecurity, shedding light on any noteworthy differences that might exist.

Cybersecurity Perspectives by Level of Education

Analysis # 1-a >> Independent Samples T-Test. Table 30 shows the Independent Samples T-Test of students’ cybersecurity perspectives by Level of Education.

Table 30

Independent Samples T-Test-Cybersecurity Perspectives by Level of Education

Cybersecurity Perspectives	***Level of Education***	***N***	***Mean***	***Std. Deviation***	***Std. Error Mean***
	Undergraduates	*336*	*3.35*	*0.67*	*0.037*
	Graduates	*245*	*3.35*	*0.69*	*0.044*

		Levene's Test for Equality of Variance				***Significance***		
Cybersecurity Perspectives		*F*	*Sig.*	*T*	*df*	*One-Sided P*	*Two-Sided P*	*Mean Difference*
	Equal Variances Assumed	*.239*	*.63*	*.137*	*579*	*.446*	*.891*	*.008*
	Equal Variances Not Assumed			*.137*	*519*	*.446*	*.891*	*.008*

Levene's test explains that there is not any difference in variances between two samples (0.625). There is not a difference in means too, so we can conclude that cybersecurity perspectives do not differ according to level of education t($_{579}$) = 0.137, p-value *0.891* (the possibility by chance) > 0.05 (α). Because there is not any significant difference, H_0 is accepted.

An independent samples t-test analysis was conducted to assess whether there were significant differences in students' cybersecurity perspectives based on their level of education. The results indicated that no significant difference was found. Consequently, a Mann Whitney U analysis was performed to investigate potential variations in specific individual items that constitute the cybersecurity perspectives scale from the survey. Two items were selected for this analysis: "E-learning platforms are a secure place where I can share my sensitive information securely" and "E-learning platforms are reliable and confidential" The Mann Whitney U test was chosen because the individual items serve as the dependent variable, and they are measured at an ordinal level. Hence, a non-parametric approach was applied.

Analysis # 1-b >> Individual Item # 2 in Cybersecurity Perspectives Using Non-Parametric Analysis/Mann Whitney U. Table 31 shows the Mann Whitney U for item#2 of the cybersecurity perspectives – "e-learning platforms are a secure place where I can share my sensitive information securely".

Table 31

Mann Whitney U Analysis–Item #2– Cybersecurity Perspectives

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.^{a,b}	Decision
1	The distribution of cybersecurity perspectives is the same across categories of students' level of education. CST #2	Independent-Samples Mann-Whitney U Test	.477	Retain the null hypothesis.

a. The significance level is .050.

b. Asymptotic significance is displayed.

Analysis # 1-c >> Individual Item # 3 in Cybersecurity Perspectives. Table 32 shows the Mann Whitney U of item#3 of cybersecurity perspectives – "E-learning platforms are reliable and confidential".

Table 32

Mann Whitney U Analysis–Item #3–Cybersecurity Perspectives

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.^{a,b}	Decision
1	The distribution of cybersecurity perspectives is the same across categories of students' level of education. CST # 3.	Independent-Samples Mann-Whitney U Test	.654	Retain the null hypothesis.

a. The significance level is .050.

b. Asymptotic significance is displayed.

Consequently, the results reveal a consistent outcome for both Mann-Whitney U tests. No significant differences were observed in students' cybersecurity perspectives regarding the individual items, specifically "E-learning platforms are a secure place where I can share my sensitive information securely" and "E-learning platforms are reliable and confidential," when considering their level of education. This outcome aligns with the findings obtained from the independent sample t-test conducted earlier.

Cybersecurity Awareness by the Discipline

Levene’s test explains the difference in variances between two samples (0.011). There is a significant difference in means too, so we can conclude that the cybersecurity awareness differs according to the discipline t ($_{238}$) = -11.25 p-value < 0.001 (the possibility by chance) < 0.05 (α). There is a significant difference. Therefore, H_0 is rejected. See Table 33 below.

Table 33

Independent Samples t-Test - Cybersecurity Awareness by Discipline

Cybersecurity Awareness	***Discipline***	***N***	***Mean***	***Std. Deviation***	***Std. Error Mean***
	Non-Computer Related	*452*	*3.19*	*0.92*	*0.043*
	Computer Related	*129*	*4.11*	*0.79*	*0.069*

		Levene’s Test for Equality of Variance		***Significance***				
Cybersecurity Awareness		*F*	*Sig.*	*t*	*df*	*One-Sided P*	*Two-Sided P*	*Mean Difference*
	Equal Variances Assumed	*6.48*	*.011*	*-10.29*	*579*	*<.001*	*<.001*	*-.92*
	Equal Variances Not Assumed			*-11.25*	*238*	*<.001*	*<.001*	*-.92*

Computer Self-Efficacy (CSE) by Discipline

Levene’s test explains that there is not any significant difference in variances among two samples (0.963). While t-test shows that there is a significant difference in the means, so we can conclude that the computer self-efficacy (CSE) differs according to the discipline t ($_{579}$) = -4.594 p-value <.001 (the possibility by chance) < 0.05 (α). There is a significant difference. Therefore, H_0 is rejected.

Table 34

Independent Samples t-Test – Computer Self-Efficacy by Discipline

Computer Self-Efficacy	***Discipline***	***N***	***Mean***	***Std. Deviation***	***Std. Error Mean***
	Non-Computer Related	*452*	*3.48*	*0.66*	*0.031*
	Computer Related	*129*	*3.78*	*0.63*	*0.055*

		Levene’s Test for Equality of Variance				***Significance***		
Computer Self-Efficacy		*F*	*Sig.*	*t*	*Df*	*One-Sided P*	*Two-Sided P*	*Mean Difference*
	Equal Variances Assumed	*.002*	*.96*	*-4.59*	*579*	*<.001*	*<.001*	*-.29*
	Equal Variances Not Assumed			*-4.72*	*215*	*<.001*	*<.001*	*-.29*

One-Way ANOVA Test

ANOVA is a statistical method used to determine whether there is a significant difference between the means of three or more groups. It is an extension of the t-test, which is used to compare the means of two groups. According to Rice (2006), the ANOVA test works by dividing the total variability in a set of data into two components: the variability between the groups and the variability within the groups. If the variability between the groups is larger than the variability within the groups, then it suggests that there is a significant difference between the means of the groups. There are several types of ANOVA tests, including one-way ANOVA, which is used when there is one independent variable, and factorial ANOVA, which is used when there are two or more independent variables (Lee & Lee, 2018).

The ANOVA test assumes several things:

1. The data is normally distributed within each group.
2. The variances of the groups are equal (homogeneity of variances).
3. The observations are independent within and between the groups.
4. The groups are randomly selected and representative of their respective populations.

If any of these assumptions are not met, the results of the ANOVA test may not be reliable. In particular, violation of the assumption of homogeneity of variances can result in the test having low power to detect true group differences or even leading to a higher risk of Type I error (false positives).

Privacy Concerns by Gender

Table 35 reveals that there is a significant difference in privacy concerns according to gender ($F_{2, 579}$ = 8.922, *p*-value < .001 < .05). Therefore, H0 is rejected because there is a difference in at least one pair of variables. The ANOVA table above provides important information about the analysis of variance conducted on the dataset. The sum of squares (SS) between groups value of 11.599 indicates the total variability or spread of the data that can be attributed to the differences between the means of the groups. This value represents the sum of the squared deviations of each group mean from the overall mean. The degrees of freedom (df) between groups is 2, which means that two groups were being compared in the analysis. The df is calculated as the number of groups minus 1, so in this case, there were three groups in total.

On the other hand, the SS within groups value of 376 represents the variability or spread of the data within each individual group. It measures how much each data point within a group deviates from its respective group mean. This value indicates the sum of the squared deviations within each group. The SS within groups provides an estimate of the variability that is not explained by the differences between the group means. It can be seen as the "error" or "noise" within each group. Both the sum of squares between groups and within groups contribute to the calculation of the F-value and its associated significance value, which are used to determine whether there are significant differences between the group means.

An ANOVA tests whether there are any significant differences among the means of three or more groups. If the overall ANOVA test is statistically significant, indicating that there are differences among the groups, additional tests may be performed to determine which specific group means differ significantly from each other. In such cases, post-hoc tests can be used, and one common post-hoc test is the independent sample t-test. This test compares the means of two groups at a time, identifying which pairs of groups differ significantly. The t-test assumes that the samples are independent, which is typically the case when comparing different subgroups within an ANOVA. In summary, one-way ANOVA is suitable for comparing more than two groups or treatments, and if significant differences are found, further investigation through multiple comparison procedures, also known as post-hoc tests or pairwise comparisons is necessary to determine the specific group differences (Bewick et al., 2004).

Table 35

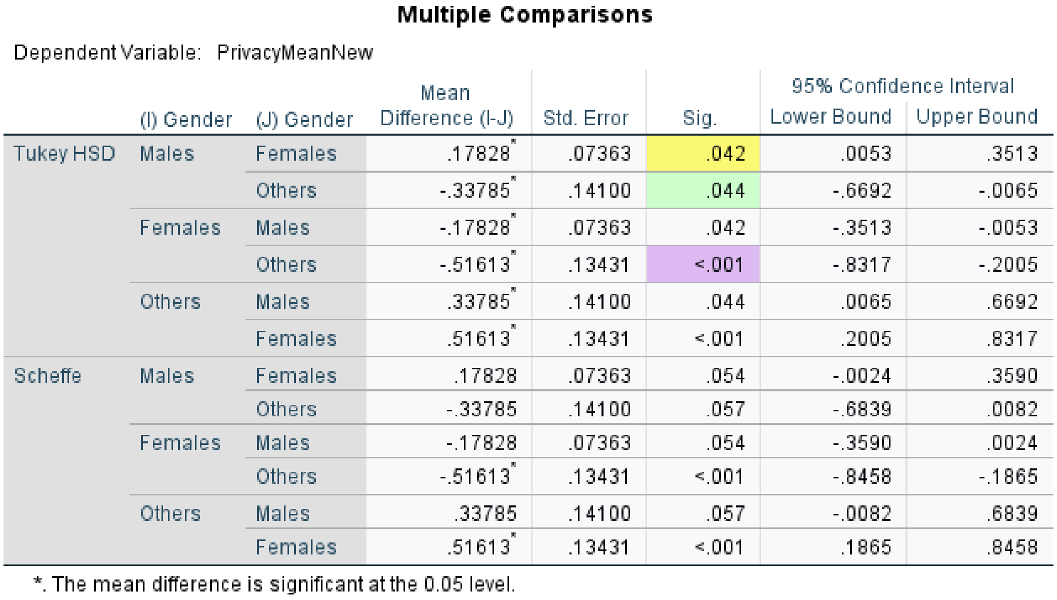
ANOVA Result

Privacy Concerns	**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig**
Between Groups	11.599	2	5.799	8.922	<.001
Within Groups	376.34	579	.65		
Total	387.94	581			

To determine which exact pair is significantly different, an independent sample t-test analysis was employed. Table 36 shows a post hoc multiple comparisons table that was prepared by conducting Tukey analysis within One-Way ANOVA. Table 36 revealed that all subgroups, “Males” and “Females,” "Males" and "Others" and "Females" and "Others" indicated the presence of significant distinctions among these sub-groups as well. Consequently, the students' privacy concerns vary based on their gender across all the gender-defined sub-groups in this study.

Table 36

Multiple Comparisons –Tukey & Scheffe



Multiple Comparisons

Dependent Variable: PrivacyMeanNew

	(I) Gender	(J) Gender	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Tukey HSD	Males	Females	.17828*	.07363	.042	.0053	.3513
		Others	-.33785*	.14100	.044	-.6692	-.0065
	Females	Males	-.17828*	.07363	.042	-.3513	-.0053
		Others	-.51613*	.13431	<.001	-.8317	-.2005
	Others	Males	.33785*	.14100	.044	.0065	.6692
		Females	.51613*	.13431	<.001	.2005	.8317
Scheffe	Males	Females	.17828	.07363	.054	-.0024	.3590
		Others	-.33785	.14100	.057	-.6839	.0082
	Females	Males	-.17828	.07363	.054	-.3590	.0024
		Others	-.51613*	.13431	<.001	-.8458	-.1865
	Others	Males	.33785	.14100	.057	-.0082	.6839
		Females	.51613*	.13431	<.001	.1865	.8458

*. The mean difference is significant at the 0.05 level.

Academic Integrity by Ethnicity

There is a significant difference in students' AI concerns according to their ethnicity ($F_{5, 576}$ = 3.452, *p*-value = 0.004 < .05). Therefore, H_0 is rejected because there is a difference in at least one pair of variables (see Table 37). According to Tukey analysis in the post hoc table located in Appendix C, there are only two groups which are significantly different. Asian starts higher (*M* = 2.89) and significant (*p* = .035) than African American as well as the second group of African American who are lower (*M* = 2.28) and significant (*p* = .004) than Arab students who are higher (*M* = 3.02) and significant (*p* = .004). See Table C2 in Appendix C to see the comparison means table with Tukey analysis and values.

Table 37

ANOVA Table–Academic Integrity Concerns by Ethnicity

Academic Integrity Concerns	**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig**
Between Groups	15.8	5	3.160	3.45	.004
Within Groups	527.17	576	.915		
Total	542.97	581			

In this study, Tables 38 and 39, respectively, offer insights into the research questions pertaining to demographics that were proposed. These tables provide answers and summaries of the results obtained from hypothesis testing conducted in relation to the demographic research questions.

Table 38

Analytical Matrix (C)–Demographics Effect on the Proposed Predictors-Results

#	Demographics Research Question	Analysis	Results
1	Do cybersecurity perspectives differ by level of education?	Independent samples t-test	No difference. Levene's test explains that there is not any difference in variances among two samples (0.625). There is not a difference in means too, so we can conclude that the cybersecurity perspectives don't differ according to the level of education *$t_{(579)}$ = 0.137 p-value is 0.891* (the possibility by chance) > 0.05 (α). There is not any significant difference. Accept H_0.
2-a & b	Do cybersecurity perspectives of students according to the individual items # 2 and 3 differ by level of education?	Non-Parametric Analysis - Mann Whitney U	There is no difference. Mann Whitney U test explains the existence of no difference in variances among two samples with *0.48 and 0.65 significance values.* There is not any difference in means among the two samples, so we can conclude that Cybersecurity perspectives don't differ according to the level of education samples. Accept H_0!
3	Do the Privacy concerns differ by gender?	One-Way ANOVA	Yes, there is a significant difference in privacy concerns according to gender among all sub-groups. ($F_{2, 579}$ = 8.922, p-value < 0.001 < 0.05. Reject H_0 and accept that there is a difference in at least one pair of variables.

Table 38 Continued

#	Demographics Research Question	Analysis	Results
4	Does cybersecurity awareness differ by discipline?	Independent Samples t-test	Levene's test explains the difference in variances between two samples (0.011). There is a significant difference in means too, so we can conclude that the cybersecurity awareness differs according to the discpline *$t_{(238)} = -11.25$ p-value <0.001* (the possibility by chance) < 0.05 (α). There is a significant difference. Reject H_0.
5	Do academic integrity concerns differ by ethnicity?	One-Way ANOVA	There is a significant difference in students' academic integrity concerns according to their ethnicity. ($F_{5, 576} = 3.452$, p-value = 0.004 < 0.05. Reject H_0 and accept that there is a difference in at least one pair of variables.
6	Does computer self-efficacy differ by discipline?	Independent Samples t-test	Levene's test explains that there is not any significant difference in variances among two samples (0.963). While t-test shows that there is a significant difference in the means, so we can conclude that the computer self-efficacy (CSE) differs according to the discipline *$t_{(579)} = -4.594$ p-value <0.001* (the possibility by chance) < 0.05 (α). There is a significant difference. Reject H_0.

Table 39

Demographics Hypotheses Testing Result

#	Alternative Hypotheses	Decision	Justification
Ha_1	There is a significant difference in the mean of students' cybersecurity perspectives by level of education.	*Rejected*	Levene's test explains that there is not any difference in variances among two samples (0.625). There is not a difference in means too, so we can conclude that the cybersecurity perspectives don't differ according to the level of education *$t_{(579)} = 0.137$ p-value is 0.891* (the possibility by chance) > 0.05 (α).
Ha_2	There is a significant difference in the mean of students' privacy concerns by gender.	*Supported*	Yes, there is a significant difference in privacy concerns according to gender. ($F_{2, 579} = 8.922$, p-value < 0.001 < 0.05. Reject H_0 and accept that there is a difference in at least one pair of variables.
Ha_3	There is a significant difference in the mean of students' cybersecurity awareness by discipline.	*Supported*	Levene's test explains the difference in variances between two samples (0.011). There is a significant difference in means too, so we can conclude that the cybersecurity awareness differs according to the discpline *$t_{(238)} = -11.25$ p-value <0.001* (the possibility by chance) < 0.05 (α). There is a significant difference. Reject H_0.
Ha_4	There is a significant difference in the mean of students' academic integrity concerns by ethnicity.	*Supported*	There is a significant difference in students' academic integrity concerns according to their ethnicity. ($F_{5, 576} = 3.452$, p-value = 0.004 < 0.05. Reject H0 and accept that there is a difference in at least one pair of variables.
Ha_5	There is a significant difference in the mean of students' computer self-efficacy by discipline.	*Supported*	Levene's test explains that there is not any significant difference in variances among two samples (0.963). While t-test shows that there is a significant difference in the means, so we can conclude that the computer self-efficacy (CSE) differs according to the discipline *$t_{(579)} = -4.594$ p-value <0.001* (the possibility by chance) < 0.05 (α). There is a significant difference. Reject H_0.

Linear and Multiple Regression

Linear regression and multiple regression are both statistical techniques employed to analyze the connection between a dependent variable and one or more independent variables. The primary distinction between the two lies in the number of independent variables incorporated within the regression model. Linear regression modeles the relationship between a dependent variable and a single independent variable, employing a straight line to represent this relationship. The objective of linear regression is to determine the line of best fit that minimizes the discrepancy between the predicted values and the actual values of the dependent variable. This line can subsequently be used to make predictions regarding the dependent variable based on the independent variable (Smith & Johnson, 2022).

Multiple regression, on the other hand, models the relationship between a dependent variable and multiple independent variables, using a plane or hyperplane to represent the relationship. The goal of multiple regression is to find the plane or hyperplane of best fit that minimizes the difference between the predicted values and the actual values of the dependent variable. This plane or hyperplane can then be used to make predictions about the dependent variable based on the independent variables (Clark & Watson, 2022).

In summary, the primary distinction between linear regression and multiple regression lies in the number of independent variables employed in the model. Linear regression involves the use of a single independent variable, whereas multiple regression incorporates two or more independent variables. Multiple regression is typically more intricate than linear regression, but it offers enhanced accuracy and utility when there exist multiple independent variables that are believed to impact the dependent variable (Johnson & Davis, 2022).

In this study, the regression model (see Tables 40-42) explains only 23% of the variation in the intention to use e-learning platforms explained by cybersecurity concerns, privacy concerns, cybersecurity awareness, academic integrity, and computer self-efficacy. The omnibus tests show we have a significant model ($F_{5,\ 576} = 34.6$, $p < .001$). Cybersecurity perspectives variable predicts students' intention to use e-learning platforms significantly ($b = .40$, $Beta = .27$, $t = 6.83$, $p <.001$) after controlling for other privacy concerns, cybersecurity awareness, academic integrity, and computer self-efficacy. For the privacy concerns variable, it seems to be insignificant independent variable to predict students' intention to use e-learning platforms ($b = .075$, $Beta = .061$, $t = 1.58$, $p = .116$) after controlling for other cybersecurity perspectives, cybersecurity awareness, academic integrity, and computer self-efficacy. Furthermore, cybersecurity awareness variable is a significant predictor of intention to use e-learning platforms ($b = .13$, $Beta = .125$, $t = 2.95$, $p =.003$) after controlling for other cybersecurity perspectives, privacy concerns, academic integrity, and computer self-efficacy. On the other hand, academic integrity concerns variable is a significant predictor of intention to use e-learning platforms in a negative direction ($b = -.221$, $Beta = -.211$, $t = -5.51$, $p <.001$) after controlling for other cybersecurity perspectives, privacy concerns, cybersecurity awareness, and computer self-efficacy. Finally, the computer self-efficacy is a significant predictor of the intention to use e-learning platforms ($b = .23$, $Beta = .152$, $t = 3.47$, $p < .001$) after controlling for other cybersecurity perspectives, privacy concerns, cybersecurity awareness, and academic integrity.

The overall correlation (multiple correlation) among this model is (R = 481%), and the total amount of variance in the dependent variable (intention to use e-learning platforms) which is explained by the associated independent variables (cybersecurity perspectives, cybersecurity awareness, AI concerns and CSE) is about 23.1% which represented by the value of R Square.

Finally, the adjusted R squared value is considered a modified version of R-squared that accounts for predictors that are not significant in a regression model. In other words, the adjusted R-squared shows whether adding additional predictors improve a regression model or not. Adjusted R squared value in the model is equal to 22.4%, adjusted R squared value and the R squared value become closer to each other based on the sample size and variability. Consequently, we can say that the overall percentage of variance in the model is 23.1% that is explained or determined by the selected predictors which are mentioned above for this model. Table 43 provides answers to the proposed basic research questions in this study.

Table 40

Regression Model

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.481[a]	.231	.224	.893

Table 41

ANOVA Table-Regression Model

Model 1	**Sum of Squares**	**Df**	**Mean Square**	**F**	**Sig**
Regression	138.07	5	27.61	34.596	<.001[b]
Residual	459.77	576	.798		
Total	597.84	581			

Table 42

Regression Model Coefficients

Model 1		***Unstandardized Coefficients***		***Standardized Coefficients***		
		B	*Std. Error*	*Beta*	*t*	*Sig.*
	(Constant)	*.940*	*.323*		*2.909*	*.004*
	Cybersecurity Perspectives	*.395*	*.058*	*.266*	*6.83*	*<.001*
	Privacy Concerns	*.075*	*.048*	*.061*	*1.575*	*.116*
	Cybersecurity Awareness	*.130*	*.044*	*.125*	*2.951*	*.003*
	Academic Integrity Concerns	*-.221*	*.040*	*-.211*	*-5.507*	*<.001*
	Computer Self-Efficacy	*.230*	*.066*	*.152*	*3.47*	*<.001*

a. Dependent Variable: Intention to Use

Table 43

Analytical Matrix (D)-Regression Result

Question	Independent/s	Dependent	Analysis	Results
Do the cybersecurity perspectives significantly predict the intention to use e-learning platforms controlling for other privacy concerns, cybersecurity awareness, academic integrity, and computer self-efficacy?	Cybersecurity perspectives Privacy concerns Cybersecurity awareness Academic integrity concerns Computer self-efficacy	Intention to use e-learning platforms	Multiple Regression	The model explains only 23% of the variation in the intention to use e-learning platforms explained by cybersecurity concerns, privacy concerns, cybersecurity awareness, academic integrity, and computer self-efficacy. The omnibus tests show we have a significant model ($F_{5, 576}$ = 34.6, p < .001). Yes, cybersecurity perspectives variable is a significant predictor of intention to use e-learning platforms (b= .40, *Beta* = .27, t = 6.83, p <.001) after controlling for other privacy concerns, cybersecurity awareness, academic integrity, and computer self-efficacy.

Table 43 Continued

Question	Independent/s	Dependent	Analysis	Results
Do the privacy concerns significantly predict the intention to use e-learning platforms controlling for other cybersecurity concerns, cybersecurity awareness, academic integrity, and computer self-efficacy?	Cybersecurity perspectives Privacy concerns Cybersecurity awareness academic integrity concerns computer self-efficacy	Intention to use e-learning platforms	Multiple Regression	No, Privacy Concerns variable is not a significant predictor of intention to use e-learning platforms (*b*= .075, *Beta* = .061, *t* = 1.58, *p* = 0.116) after controlling for other cybersecurity concerns, cybersecurity awareness, academic integrity, and computer self-efficacy.
Does the cybersecurity awareness significantly predict the intention to use e-learning platforms controlling for other cybersecurity concerns, privacy concerns, academic integrity, and computer self-efficacy?	Cybersecurity perspectives Privacy concerns cybersecurity awareness academic integrity concerns computer self-efficacy	Intention to use e-learning platforms	Multiple Regression	Yes, the Cybersecurity Awareness variable is a significant predictor of intention to use e-learning platforms (*b*= .13, *Beta* = .125, *t* = 2.95, *p* =.003) after controlling for other cybersecurity concerns, privacy concerns, academic integrity, and computer self-efficacy.

Table 43 Continued

Question	Independent/s	Dependent	Analysis	Results
Do the academic integrity concerns significantly predict the intention to use e-learning platforms controlling for other cybersecurity concerns, privacy concerns, cybersecurity awareness, and computer self-efficacy?	Cybersecurity perspectives Privacy concerns cybersecurity awareness academic integrity concerns computer self-efficacy	Intention to use e-learning platforms	Multiple Regression	Yes, the Academic Integrity Concerns variable is a significant predictor of intention to use e-learning platforms (*b*= -.221, *Beta* = -.211, *t* = -5.51, *p* <.001) after controlling for other cybersecurity concerns, privacy concerns, cybersecurity awareness, and computer self-efficacy.
Does computer self-efficacy significantly predict the intention to use e-learning platforms controlling for other cybersecurity concerns, privacy concerns, cybersecurity awareness, and academic integrity?	Cybersecurity perspectives Privacy concerns cybersecurity awareness academic integrity concerns computer self-efficacy	Intention to use e-learning platforms	Multiple Regression	Yes, the Computer Self-Efficacy is a significant predictor of the intention to use e-learning platforms (*b*= .23, *Beta* = .152, *t* = 3.47, *p* <.001) after controlling for other cybersecurity concerns, privacy concerns, cybersecurity awareness, and academic integrity.

Summary of Chapter Four

The collected data were analyzed using SPSS 28, and hypotheses were tested with a significance level of 0.05. Out of 6,800 distributed surveys, 590 responses were received and 582 were included in the final sample after data cleaning. The findings indicate that cybersecurity perspectives, cybersecurity awareness, AI concerns, and CSE significantly explain students' intention to use e-learning platforms.

According to the comparison analyses, all questions related to demographics are supported except for the question regarding the disparity in students' cybersecurity perspectives based on their level of education. The independent samples t-test indicates that there is no significant difference in students’ cybersecurity perspectives across different levels of education. However, the results of the one-way ANOVA and other independent samples t-tests reveal significant differences among the compared samples in various aspects. These differences include privacy concerns by gender, cybersecurity awareness by discipline, AI concerns by ethnicity, and CSE by discipline.

In regression analysis, R represents the correlation coefficient, which measures the strength and direction of the linear relationship between the independent variables and the dependent variable. The regression model for this study shows the value of R is 0.48. This indicates a moderate positive correlation between the independent variables and the dependent variable. R-squared (R^2) is a statistical measure that represents the proportion of the variance in the dependent variable that is explained by the independent variables in the regression model. The model has R^2 value of 0.23, which means that approximately 23% of the variability in the dependent variable can be explained by the independent variables included in the model. The remaining 77% of the variability is unexplained and may be attributed to other factors not considered in the model or random variation. Adjusted R-squared is a modified version of R^2 that takes into account the number of predictors in the model and adjusts the value accordingly. It penalizes the addition of unnecessary variables that do not significantly contribute to explaining the variance in the dependent variable. In your case, the adjusted R^2 is 0.224, which is slightly lower than the R^2. This suggests that the independent variables in the model are providing a modest amount of explanatory power, considering the number of predictors included.

Chapter Five: Conclusion

This research focuses on the challenges faced by students who engage in e-learning platforms. The main areas of concern examined in this dissertation were cybersecurity perspectives, privacy concerns, cybersecurity awareness, AI concerns, and CSE. The study aimed to understand the impact of these factors on students' intention to use e-learning platforms even after the COVID-19 pandemic. As university students spend significant time online, using computers for various activities such as attending online courses, submitting assignments, communicating with instructors and peers, and taking online exams (Bailey & Lee, 2020), they are particularly vulnerable to cyberattacks. In addition, privacy emerges as a prominent concern for students in the academic context. Students encounter substantial privacy issues as instructors rely on emails and electronic platforms to share sensitive information like names, grades, meeting locations, and intellectual property. Furthermore, online proctored exams pose a threat to students' privacy, as students may experience discomfort and unease due to the monitoring and observation involved during the examination process (Balash et al., 2021).

Additionally, this research highlighted the imminent threat of data loss for students in the context of e-learning. The loss or theft of their devices like computers, flash drives, and phones poses risks to their privacy, confidentiality, and anonymity. A hacking attack or unauthorized intrusion can further compromise student accounts and result in data loss. Insufficient awareness and knowledge of cybersecurity threats may prevent students from adequately protecting their devices from hackers who may impersonate other students (Ulven & Wangen, 2021). Additionally, in online classes, assignments such as interactive discussion threads expose students' personal ideas and thoughts to unauthorized access and sharing, posing a threat to their intellectual property. Therefore, it is crucial to explore students' intention to use e-learning platforms within the context of cybersecurity. This dissertation aimed to determine students' acceptance levels regarding the adoption of these platforms based on five proposed predictors: cybersecurity perspectives, privacy concerns, cybersecurity awareness, CSE, and AI concerns. The research aimed to provide a better understanding of essential concepts and critical risks in digital education while raising awareness among students.

In this research, TAM3 model was utilized as the methodological framework to investigate how cybersecurity perspectives, privacy concerns, cybersecurity awareness, AI concerns, and CSE, influence students' perceptions and intentions towards using e-learning platforms in the future. Multiple regression analysis was conducted to answer the research questions for this study. The analysis indicated that not all independent variables demonstrated significant predictive power in the model. Specifically, the variables of cybersecurity perspectives, cybersecurity awareness, AI concerns, and CSE were found to be significant predictors of the dependent variable, ITU. However, the independent variable of privacy concerns exhibited a non-significant negative impact when predicting ITU.

Result of Hypotheses Testing

Hypothesis testing, a crucial tool in statistical analysis, plays a significant role across various fields by enabling informed decision-making and drawing conclusions based on data (Page & Satake, 2017). Researchers and analysts rely on hypothesis testing to assess theories, explore research questions, and make well-founded decisions based on evidence. It serves as a fundamental technique that aids in the evaluation and validation of hypotheses, ensuring rigorous and reliable analysis. Pearson correlation analysis was utilized to test hypotheses and determine which hypotheses were supported and which ones were rejected.

Basic Research Questions Answers

Following the performance of multiple linear regression analysis, the findings indicate that only four independent variables hold significance in elucidating the dependent variable of this study, namely the intention to use e-learning platforms. Broadly speaking, the noteworthy predictors for explaining students' intention to use e-learning platforms in the future are cybersecurity perspectives, cybersecurity awareness, AI concerns, and CSE.

The regression model explains only 23% of the variation in the intention to use e-learning platforms explained by cybersecurity concerns, privacy concerns, cybersecurity awareness, academic integrity, and computer self-efficacy. The omnibus tests show we have a significant model ($F_{5, 576 =}$ 34.6, $p < .001$).

Research Question One: To What Extent Do Students' Cybersecurity Perspectives Affect Their Intention to Use E-Learning Platforms?

The Cybersecurity Perspectives variable is a significant predictor of intention to use e-learning platforms (b= .40, *Beta* = .27, t = 6.83, $p < .001$) after controlling for other privacy concerns, cybersecurity awareness, AI concerns, and CSE.

Research Question Two: To What Extent Do Students' Privacy Concerns Affect Their Intention to Use E-Learning Platforms?

The Privacy Concerns variable is not a significant predictor of intention to use e-learning platforms (b= .075, *Beta* = .061, t = 1.58, p = 0.116) after controlling for other cybersecurity perspectives, cybersecurity awareness, AI concerns, and CSE.

Research Question Three: To What Extent Does Students' Cybersecurity Awareness Affect Their Intention to Use E-Learning Platforms?

The Cybersecurity Awareness variable is a significant predictor of intention to use e-learning platforms (*b*= .13, *Beta* = .125, *t* = 2.95, *p* =.003) after controlling for other cybersecurity perspectives, privacy concerns, AI concerns, and CSE.

Research Question Four: To What Extent Do Students' Academic Integrity Concerns Affect Their Intention to Use E-Learning Platforms?

The AI Concerns variable is a significant predictor of intention to use e-learning platforms (*b*= -.221, *Beta* = -.211, *t* = -5.51, *p* < .001) after controlling for other cybersecurity perspectives, privacy concerns, cybersecurity awareness, and CSE.

Research Question Five: To What Extent Does Students' Computer Self-Efficacy Affect Their Intention to Use E-Learning Platforms?

CSE is a significant predictor of the intention to use e-learning platforms (*b*= .23, *Beta* = .152, *t* = 3.47, *p* < .001) after controlling for other cybersecurity perspectives, privacy concerns, cybersecurity awareness, and AI concerns.

Final Multiple Regression Model

For this study the observed regression equation is to be as the following:

Intention to Use e-Learning Platforms = β0 + β1* Cybersecurity Perspectives - β3 * Academic Integrity concerns + β4 * Cybersecurity Awareness + β5 * Computer Self-Efficacy+ εi

Intention to Use e-Learning Platforms = 0.94 + 0.40 * Cybersecurity Perspectives – 0.22 * Academic Integrity concerns + 0.13 * Cybersecurity Awareness + 0.23 * Computer Self-Efficacy+ εi

Meaning of Each Component in the Final Regression Model

The followings are the main components that building the regression model for this study. First, the Intercept (0.94): This is the constant term or the baseline value when all the independent variables (Cybersecurity Perspectives, AI Concerns, Cybersecurity Awareness, and CSE) are zero. In this case, when all the predictors are absent, the predicted value of Intention to Use e-Learning Platforms would be 0.94. Second, Cybersecurity Perspectives (0.40): This coefficient indicates the strength and direction of the relationship between Cybersecurity Perspectives and the Intention to Use e-Learning Platforms. A one-unit increase in Cybersecurity Perspectives is associated with a predicted increase of 0.40 in the Intention to Use e-Learning Platforms, assuming the other variables remain constant. Third, AI Concerns (-0.22): This coefficient represents the relationship between AI Concerns and the Intention to Use e-Learning Platforms. A one-unit increase in AI Concerns is associated with a predicted decrease of 0.22 in the Intention to Use e-Learning Platforms, assuming the other variables remain constant. Fourth, Cybersecurity Awareness (0.13): This coefficient represents the relationship between Cybersecurity Awareness and the Intention to Use e-Learning Platforms. A one-unit increase in Cybersecurity Awareness is associated with a predicted increase of 0.13 in the Intention to Use e-Learning Platforms, assuming the other variables remain constant. Fifth, CSE (0.23): This coefficient represents the relationship between CSE and the Intention to Use e-Learning Platforms. A one-unit increase in CSE is associated with a predicted increase of 0.23 in the Intention to Use e-Learning Platforms, assuming the other variables remain constant. Finally, εi: This term represents the error or residual term, which captures the unexplained variability in the Intention to Use e-Learning Platforms that cannot be accounted for by the independent variables. It accounts for any random or unmeasured factors that affect the outcome.

In summary, the regression model suggests that the Intention to Use e-Learning Platforms is influenced by various factors, including positive influences from Cybersecurity Perspectives, Cybersecurity Awareness, and CSE, and a negative influence from AI Concerns. The model allows us to estimate the impact of these variables on the Intention to Use e-Learning Platforms and make predictions based on their values.

Demographics Research Questions Answers

This section addresses the overarching inquiry of how demographics influence the five proposed predictors. Subsequently, a combination of parametric analyses, such as independent samples t-tests and one-way ANOVA, along with non-parametric analyses, such as Mann-Whitney U test, were conducted to address specific sub-questions. The employment of these statistical tests, available within the mean comparisons functions in SPSS, allowed for comprehensive examination of questions involving ordinal dependent variables.

Question One: Do Cybersecurity Perspectives Differ by Level of Education?

The result shows there is not any significant difference. Levene's test explains that there is not any difference in variances among two samples (0.625). There is not a difference in means too, so we can conclude that the cybersecurity perspectives don't differ according to the level of education $t\ (_{579}) = 0.137$ *p-value is 0.891* (the possibility by chance) > 0.05 (α). There is not any significant difference. Thus H_0 is accepted.

Question Two: Do Privacy Concerns Differ by Gender?

The result shows there is a significant difference in privacy concerns according to gender among all sub-groups. ($F_{2,\, 579} = 8.922$, *p-value* < 0.001 < 0.05. Thus, H_0 is rejected because there is a difference in at least one pair of variables.

Question Three: Does Cybersecurity Awareness Differ by Discipline?

Levene's test explains the difference in variances between two samples (0.011). There is a significant difference in means too, so we can conclude that the cybersecurity awareness differs according to the discipline *t* $(_{238})$ *= -11.25 p-value <0.001* (the possibility by chance) < 0.05 (α). There is a significant difference. Thus, H_0 is rejected.

Question Four: Do AI concerns Differ by Ethnicity?

There is a significant difference in students' AI concerns according to their ethnicity. ($F_{5, 576}$ = 3.452, *p-value* = 0.004 < 0.05. Thus, H_0 is rejected because there is a difference in at least one pair of variables.

Question Five: Does CSE Differ by Discipline?

Levene's test explains that there is not any significant difference in variances among two samples (0.963). While t-test shows that there is a significant difference in the means, so we can conclude that the CSE differs according to the discipline *t* $(_{579})$ *= -4.594 p-value < .001* (the possibility by chance) < 0.05 (α). There is a significant difference. Therefore, H_0 is rejected.

Study Limitations

The study encountered several limitations that need to be acknowledged. Firstly, there was a low response rate during the initial distribution of the online survey link. Additionally, a second reminder had to be sent to the participants as they were not regularly checking their emich email. As a result, there was a delay in collecting data because of the low response. Secondly, due to the time constraints inherent in a dissertation project, all requirements for submitting the final draft had to be met by a specific deadline. Lastly, it is important to recognize that these limitations may have implications for the generalizability and completeness of the study's findings.

Furthermore, it is crucial to acknowledge that another factor contributing to the limitations is the uncertain honesty of participants' responses. Since the survey relied on self-reported data, there is always the possibility of response bias or participants not providing completely accurate information. This uncertainty in the honesty of responses may affect the reliability and validity of the study's findings. Finally, another limitation of this research is that the model only accounts for 23% of the observed variation. It raises questions about the presence of additional variables that were not included in the analysis, which could potentially explain a larger portion of the variation. For instance, factors such as prior experiences might play a significant role, although their effects were not considered in this study. While the results are well-explained, the limited explanatory power of the model leaves room for further investigation and consideration of other influential factors in future research.

Overall, these limitations, including the low response rate, delay in collecting the data from the required sample size, time constraints, the uncertainty factor of participant responses, and the variability percentage of the regression model that should be considered when conducting any future research work.

Future Research Work Directions

In this section, the researcher outlines potential avenues for future research that could build upon the findings and contribute to the further advancement of the field. These directions are intended to inspire and guide future researchers in their exploration of the topic.

A potential future research extension could involve utilizing the same survey deployed in this research project and distributing it to another university that also utilizes the same e-learning platform (Canvas) as EMU. This extended study could aim to compare the survey results based on a new factor, namely the region or culture, such as Jordan.

Additionally, a second research direction could explore a comparative analysis of students' perspectives between those who use different e-learning platforms, such as Blackboard or Moodle, within the context of the USA. This investigation could offer valuable insights into the variations in perceptions and experiences based on the specific e-learning platform employed.

Furthermore, a valuable approach would be to conduct new qualitative research to gather insights directly from students at EMU. This qualitative study could focus on identifying the factors that students believe strongly influence their intentions to use e-learning platforms. By incorporating students' responses, a robust framework could be developed through coding and analyzing the data. This framework could provide new patterns and variables that can inform a subsequent study, further supporting the existing framework developed in this current study.

Research Implications

This research has examined numerous articles in the field of cybersecurity and e-learning platforms to understand their implications. The reviewed articles shed light on the adoption of e-learning platforms from a cybersecurity perspective and provided definitions and illustrations of cybersecurity-related aspects. This dissertation explains each of the five proposed factors in detail and presents important terms in an organized table for clarity. Summarized tables are included throughout the dissertation to facilitate understanding for non-experts in the domain of cybersecurity. Among the articles reviewed, it was discovered that only a limited number of studies have utilized TAM as a framework to investigate the adoption of e-learning platforms from a cybersecurity perspective. This strengthens the significance and impact of this dissertation. TAM has been expanded in this study to include the five predictors as external variables, thereby examining their combined influence. It is worth mentioning that a section of this dissertation has recently been published in the IJSRMS and was available in the journal online edition in November 2022. This dissertation aimed to assist IT staff in creating and maintaining a high-quality online course platform that better meets the needs of students and enhances their satisfaction (Chang et al., 2022). Furthermore, the findings of this study will be valuable to researchers, administrators, and planners in educational institutions, as they provide insights into the current state of e-learning platforms and emphasize the importance of cybersecurity awareness in addressing cyber threats (Dash & Ansari, 2022).

Summary of Chapter Five

The findings of this research indicate that cybersecurity perspectives, cybersecurity awareness, AI concerns, and CSE significantly contribute to students' intention to use e-learning platforms, as supported by a p-value below 0.05. However, privacy concerns do not significantly impact predicting students' intention to use e-learning platforms, with a p-value above 0.05.

This study sheds light on the importance of cybersecurity in the context of e-learning platforms, particularly in safeguarding personal information and data from unauthorized access, use, or disclosure. The four aforementioned independent variables—Cybersecurity Perspectives, Cybersecurity Awareness, AI Concerns, and CSE—emerge as crucial factors influencing students' intention to use e-learning platforms. AI Concerns refer to the ethical conduct and honesty of students in academic activities, encompassing assignments, exams, and research. Research findings affirm that academic integrity significantly affects students' intention to use e-learning platforms, with a p-value below 0.05. Similarly, cybersecurity awareness, which involves educating students about cybersecurity importance and associated risks, significantly influences students' intention to use e-learning platforms, supported by a p-value below 0.05. Moreover, CSE, representing students' confidence in effectively utilizing computers and related technology, is a significant predictor of students' intention to use e-learning platforms, with a p-value below 0.05. In summary, cybersecurity perspectives, cybersecurity awareness, AI concerns, and CSE emerge as significant predictors explaining students' intention to use e-learning platforms at EMU. These factors hold paramount importance in ensuring the safety, security, and effective utilization of students' personal information, data, and academic activities.

References

Abayomi, A. A. (2020). Applying space transition theory to cybercrime: A theoretical analysis of revenge pornography in the 21st century. *International Journal of Innovative Science and Research Technology, 5*(11), 631-637.

Abbad, M. M. (2021). Using the UTAUT model to understand students' usage of e-learning systems in developing countries. *Education and Information Technologies, 26*(6), 7205-7224.

Achim, N., & Al Kassim, A. (2015). Computer usage: The impact of computer anxiety and computer self-efficacy. *Procedia-Social and Behavioral Sciences, 172*(2015), 701-708.

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived usefulness, ease of use, and usage of information technology: A replication. *MIS Quarterly, 16*(2), 227-247.

Adnan, M., & Anwar, K. (2020). Online learning amid the COVID-19 pandemic: Students' perspectives. *Online Submission, 2*(1), 45-51.

Agustina, P. Z. R., & Cheng, T. H. (2020). How students' perspectives about online learning amid the COVID-19 pandemic? *Studies in Learning and Teaching, 1*(3), 133-139.

Ahmad, S., Islam, M., & Amin, M. (2020). A study of Pakistani students' perceptions about academic dishonesty at university level. *Journal of Research & Reflections in Education, 14*(1), 81-92.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology, 22*(5), 453-474.

Alam, M. M., Ahmad, N., Naveed, Q. N., Patel, A., Abohashrh, M., & Khaleel, M. A. (2021). E-learning services to achieve sustainable learning and academic performance: An empirical study. *Sustainability*, *13*(5), 2653.

Alammary, A., Alshaikh, M., & Alhogail, A. (2021). The impact of the COVID-19 pandemic on the adoption of e-learning among academics in Saudi Arabia. *Behaviour & Information Technology*, 1-23.

Alassafi, M. O. (2022). E-learning intention material using TAM: A case study. *Materials Today: Proceedings*, *61*, 873-877.

Al Bashaireh, R. (2023). Cloud-based e-learning: Concepts, and its beneficial role during the COVID-19 dilemma. *In Proceedings of Seventh International Congress on Information and Communication Technology* (pp. 491-505). Springer, Singapore.

Aldhahi, M. I., Alqahtani, A. S., Baattaiah, B. A., & Al-Mohammed, H. I. (2022). Exploring the relationship between students' learning satisfaction and self-efficacy during the emergency transition to remote learning amid the coronavirus pandemic: A cross-sectional study. *Education and Information Technologies, 27*(1), 1323-1340.

Alessio, H. M., Malay, N., Maurer, K., Bailer, A. J., & Rubin, B. (2018). Interaction of proctoring and student major on online test performance. *International Review of Research in Open and Distributed Learning, 19*(5), 166-185.

Alexei, L. A., & Alexei, A. (2021). Analysis of IoT security issues used in higher education institutions. *International Journal of Mathematics and Computer Research, 5,* 2277-2286.

Al-Fraihat, D., Joy, M., & Sinclair, J. (2020). Evaluating e-learning systems success: An empirical study. *Computers in Human Behavior*, *102*, 67-86.

Algahtani, A. (2011). *Evaluating the effectiveness of the e-learning experience in some universities in Saudi Arabia from male students' perceptions* [Unpublished doctoral dissertation]. Durham University.

Ali, R., & Zafar, H. (2017). A security and privacy framework for e-learning. *International Journal for E-Learning Security*, *7*(2), 556–566.

Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C., & Fonseca, D. (2021). Privacy and e-learning: A pending task. *Sustainability*, *13*(16), 9206.

Alleyne, P., & Phillips, K. (2011). Exploring academic dishonesty among university students in Barbados: An extension to the theory of planned behaviour. *Journal of Academic Ethics*, *9*(4), 323-338.

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*, 5261-5280.

Almaiah, M. A., & Alyoussef, I. Y. (2019). Analysis of the effect of course design, course content support, course assessment and instructor characteristics on the actual use of e-learning system. *IEEE Access*, *7*, 171907-171922. doi:10.1109/ACCESS.2019.2956349.

Alotaibi, R. S., & Alshahrani, S. M. (2022). An extended DeLone and McLean's model to determine the success factors of e-learning platform. *PeerJ Computer Science*, *8*, e876.

Alqahtani, A. Y., & Rajkhan, A. A. (2020). E-learning critical success factors during the COVID-19 pandemic: A comprehensive analysis of e-learning managerial perspectives. *Education Sciences*, *10*(9), 216.

Al-Quraan, H., Abu-Shanab, E., Banitaan, S., & Al-Tarawneh, H. (2017). Motivations for using social media: Comparative study based on cultural differences between American and

Jordanian students. *International Journal of Social Media and Interactive Learning Environments, 5*(1), 48-61.

Alquran, H., & Ferdousi, B. (2022). Effect of cybersecurity, privacy and academic integrity concerns on assessment in e-learning environment. *International Journal of Scientific Research in Multidisciplinary Studies, 8*(11), 11-18.

Al-Rahmi, W. M., Yahaya, N., Aldraiweesh, A. A., Alamri, M. M., Aljarboa, N. A., Alturki, U., & Aljeraiwi, A. A. (2019). Integrating technology acceptance model with innovation diffusion theory: An empirical investigation on students' intention to use e-learning systems. *IEEE Access, 7,* 26797-26809. doi: 10.1109/ACCESS.2019.2899368.

Altameemi, A. F., & Al-Slehat, Z. A. F. (2021). Exploring the students' behavior intentions to adopt e-learning technology: A survey study based on COVID-19 crisis. *International Journal of Business and Management*, *16*(6), 31-41.

Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., & Hamdi, M. (2020). A survey on security and privacy issues in edge-computing-assisted internet of things. *IEEE Internet of Things Journal, 8*(6), 4004-4022.

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

Ampuni, S., Kautsari, N., Maharani, M., Kuswardani, S., & Buwono, S. B. S. (2020). Academic dishonesty in Indonesian college students: An investigation from a moral psychology perspective. *Journal of Academic Ethics*, *18*(4), 395-417.

Ansong-Gyimah, K. (2020). Students' perceptions and continuous intention to use e-learning systems: The case of Google classroom. *International Journal of Emerging Technologies in Learning*, *15*(11), 236-244.

Arbaugh, J. B. (2010). Multi-disciplinary and program-level research in online business education. *Online and Blended Business Education for the 21st Century*, 19-46.

Arshad, I., Zahid, H., Umer, S., Khan, S. Y., Sarki, I. H., & Yaseen, M. N. (2021). Academic dishonesty among higher education students in Pakistan. *Elementary Education Online*, *20*(5), 5334-5345.

Astalini, A., Darmaji, D., Kurniawan, W., Anwar, K., & Kurniawan, D.A. (2019). Effectiveness of using e-module and e-assessment. *International Journal of Interactive Mobile Technologies*, *13*(9), 21-39. https://doi.org/10.3991/ijim.v13i09.11016

Assarut, N., Bunaramrueang, P., & Kowpatanakit, P. (2019). Clustering cyberspace population and the tendency to commit cyber crime: A quantitative application of space transition theory. *International Journal of Cyber Criminology*, *13*(1), 84–100.

Azis, Y. M., & Leatemia, M. (2021). The effectiveness of e-learning, learning styles, prior knowledge, and internet self-efficacy in business mathematics courses. *Kreano, Jurnal Matematika Kreatif-Inovatif, 12*(2), 353-364.

Azizi, Z., Rezai, A., Namaziandost, E., & Tilwani, S. A. (2022). The role of computer self-efficacy in high school students’ e-learning anxiety: A mixed-methods study. *Contemporary Educational Technology*, *14*(2), ep356.

Bailey, D. R., & Lee, A. R. (2020). Learning from experience in the midst of COVID-19: Benefits, challenges, and strategies in online teaching. *Computer-Assisted Language Learning Electronic Journal*, *21*(2), 178-198.

Balash, D. G., Kim, D., Shaibekova, D., Fainchtein, R. A., Sherr, M., & Aviv, A. J. (2021). Examining the examiners: Students' privacy and security perceptions of online proctoring services. *In 17th Symposium on Usable Privacy and Security* (pp. 633-652). Ethyca. https://www.usenix.org/conference/soups2021/presentation/balash

Bandara, I., Ioras, F, & Maher, K. (2014). Cyber security concerns in e-learning education. In *Proceedings of ICERI2014 Conference,* (pp.728-734). *IATED.*

Banes, V., & Ravariu, C. (2022). Authentication methods with a high degree of security in accessing Moodle e-learning platform. In *Interactive mobile communication, technologies and learning: 411*. (pp. 951-961). Springer. https://doi.org/10.1007/978-3-030-96296-8_86

Bem, S. L. (1981). The BSRI and gender schema theory: A reply to Spence and Helmreich. *Psychological Review, 88(*4), 369-371. https://doi.org/10.1037/0033-295X.88.4.369

Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y., & Shinoda, Y. (2019). Supporting cybersecurity education and training via LMS integration: CyLMS. *Education and Information Technologies, 24*(6), 3619-3643. http://dx.doi.org.ezproxy.emich.edu/10.1007/s10639-019-09942-y

Bewick, V., Cheek, L., & Ball, J. (2004). Statistics review 9: One-way analysis of variance. *Critical Care, 8*(2), 130-136.

Blau, I., Goldberg, S., Friedman, A., & Eshet-Alkalai, Y. (2021). Violation of digital and analog academic integrity through the eyes of faculty members and students: Do institutional role and technology change ethical perspectives? *Journal of Computing in Higher Education*, *33*(1), 157-187.

Braun, M. T. (2013). Obstacles to social networking website use among older adults. *Computers in Human Behavior*, *29*(3), 673-680.

Bubou, G., & Job, G. (2021). Benefits, challenges and prospects of integrating e-learning into Nigerian tertiary institutions: A mini review. *International Journal of Education and Development Using Information and Communication Technology*, *17*(3), 6-18.

Buja, A. G. (2021). Cyber security features for national e-learning policy. *Turkish Journal of Computer and Mathematics Education, 12*(5), 1729-1735.

Bujaki, M., Lento, C., & Sayed, N. (2019). Utilizing professional accounting concepts to understand and respond to academic dishonesty in accounting programs. *Journal of Accounting Education, 47*(0748-5751), 28-47.

Burgason, K. A., Sefiha, O., & Briggs, L. (2019). Cheating is in the eye of the beholder: An evolving understanding of academic misconduct. *Innovative Higher Education, 44*(3), 203-218.

Burton-Jones, A., & Hubona, G. S. (2006). The mediation of external variables in the technology acceptance model. *Information & Management, 43*(6), 706-717. http://dx.doi.org/10.1016/j.im.2006.03.007

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis, 42*(8), 1643-1669.

Chai, L., Xu, J., & Li, S. (2022). Investigating the intention to adopt telecommuting during COVID-19 outbreak: An integration of TAM and TPB with risk perception. *International Journal of Human–Computer Interaction*, *26*, 1-11. https://doi.org/10.1080/10447318. 2022.2098906.

Chang, V., Liu, M., Xu, Q. A., & Xiong, C. (2022). Factors affecting student satisfaction in e-learning. *International Journal of Business and Systems Research*, *16*(4), 401-422.

Charlesworth, M., & Sewry, D. (2009). Ethical theories and computer ethics. In *Handbook of research on technoethics*. (pp.186-204). IGI Global.

Chao, C. M. (2019). Factors determining the behavioral intention to use mobile learning: An application and extension of the UTAUT model. *Frontiers in psychology*, *10*, 1652. https://doi.org/10.3389/fpsyg.2019.01652

Chibisa, A., Tshabalala, M. G., & Maphalala, M. C. (2021). Pre-service teachers' computer self-efficacy and the use of computers. *International Journal of Learning, Teaching and Educational Research, 20*(11), 325-345.

Chopra, M. A., & Chopra, M. A. (2016). Security threats and remedies in e-learning system. *International Journal of Computer Science and Telecommunications*, *7*(7), 6-10.

Chopra, G., & Madan, P. (2021). Role of potential self-efficacy on e-learning effectiveness: A gender-specific moderated mediation model. *International Journal of Learning and Change, 13*(2), 190-217.

Choudhury, S., & Pattnaik, S. (2020). Emerging themes in e-learning: A review from the stakeholders' perspective. *Computers & Education*, *144*, 103657.

Christen, M., Gordijn, B., & Loi, M. (2020). The ethics of cybersecurity. In *The International Library of Ethics, Law and Technology* (Vol. 21, pp. 384). Springer International Publishing.

Chuttur, M. (2009). Overview of the technology acceptance model: Origins, developments and future directions. *Working Papers on Information Systems, 9*(37), 9-37.

Claar, C., Portolese Dias, L., & Shields, R. (2014). Student acceptance of learning management systems: a study on demographics. *Issues in Information Systems*, *15*(1), 409-417.

Clark, A. L., & Watson, R. J. (2022). Exploring the application of multiple regression in predictive modeling: A comparative analysis. *Journal of Statistical Analysis, 34*(2), 78-96. https://doi.org/10.1080/12345678.2022.123456

Clark, J.G., Beebe, N.L., Williams, K. and Shepherd, L. (2009). Security and privacy governance: Criteria for systems design. *Journal of Information Privacy and Security, 5*(4), 3-30.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Routledge Academic..

Coman, C., Țîru, L. G., Meseșan-Schmitz, L., Stanciu, C., & Bularca, M. C. (2020). Online teaching and learning in higher education during the coronavirus pandemic: Students' perspective. *Sustainability*, *12*(24), 10367.

Compeau, D. R., & Higgins, C. A. (1995). "Computer self-efficacy: Development of a measure and initial test." *MIS Quarterly*, *19*(2), 189-211.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review. *Computers in Industry, 137*, 103614. Digital Object Identifier 10.1109/ACCESS.2022.3223370

Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy. *International Research Journal of Engineering and Technology*, *9*(4), 2395-0072.

Davis, F. D. (1989). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, 38*(3), 475-487.

Dawson, P. (2020). *Defending assessment security in a digital world: Preventing e-cheating and supporting academic integrity in higher education*. Routledge.

Devi, B., Rao, K., Setty, S., & Rao, M. (2013). Disaster prediction system using IBM SPSS data mining tool. *International Journal of Engineering Trends and Technology (IJETT), 4*(2), 3352-3357.

Di Giacomo, D., Guerra, F., Perilli, E., & Ranieri, J. (2020). Technophobia as emerging risk factor in aging: Investigation on computer anxiety dimension. *Health Psychology Research*, *8*(1), 8207. doi: 10.4081/hpr.2020.8207

Dong, Y., Xu, C., Chai, C. S., & Zhai, X. (2020). Exploring the structural relationship among teachers' technostress, technological pedagogical content knowledge (TPACK), computer self-efficacy and school support. *The Asia-Pacific Education Researcher*, *29*(2), 147-157.

Eibl, C. J. (2009, May). Privacy and confidentiality in e-learning systems. In *2009 Fourth International Conference on Internet and Web Applications and Services* (pp. 638-642). IEEE.

El Andaloussi, Z., Benbba, B., & Kamal, S. (2022). Exploring the encgt business school students' perceptions toward e-learning during the COVID-19 pandemic: A quantitative descriptive study. *Ijtm International Journal of Trade And Management, 1*(1), 27-40.

El-Bassiouny, D., & El-Bassiouny, N. (2020). The challenge of online privacy preservation in Muslim-majority countries during the COVID-19 pandemic. *Journal of Islamic Marketing*, *12*(3), 622-626.

El Tantawi, M.M., Abdelsalam, M.M., Mourady, A.M. and Elrifae, I.M. (2015). E-assessment in a limited-resources dental school using an open-source learning management system. *Journal of Dental Education, 79*, 571-583.

Eastern Michigan University. *About EMU*. https://www.emich.edu/about/index.php

Emerson, R. W. (2015). Convenience sampling, random sampling, and snowball sampling: How does sampling affect the validity of research? *Journal of Visual Impairment & Blindness, 109*(2), 164-168.

Ertmer, P. A., Evenbeck, E., Cennamo, K. S., & Lehman, J. D. (1994). Enhancing self-efficacy for computer technologies through the use of positive classroom experiences. *Educational Technology Research and Development*, *42*(3), 45-62.

Espinha Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2020). Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity, 3*(1), 1-23.

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, *58*(2), 102468.

Estriegana, R., Medina, J., Robina, R., & Barchino, R. (2021, June). Virtual learning environment to encourage students' relationships and cooperative competence acquisition. In *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education (Vol. 1,* pp. 53-59).

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4.

Farid, S., Alam, M., Qaiser, G., Haq, A. A. U., & Itmazi, J. (2017). Security threats and measures in e-learning in Pakistan: A review. *Technical Journal of University of Engineering & Technology Taxila*, *22*(3), 98-107.

Ferdousi, B. (2019). The effect of computer self-efficacy and attitude on undergraduate students' intention to use emerging technology in classroom learning. *Journal of Computer Sciences and Applications, 7*(1), 50-55.

Ferdousi, B. (2020, August). Data security concerns and consumers' trust in online business. In *5th NA International Conference on Industrial Engineering and Operations Management Detroit*. Michigan, USA. http://www.ieomsociety.org/detroit2020/papers/480.pdf

Fishbein, M., Jaccard, J., Davidson, A. R., Ajzen, I., & Loken, B. (1980). *Predicting and understanding family planning behaviors in understanding attitudes and predicting social behavior*. Prentice Hall.

Furnell, S. M., & Karweni, T. (2001). Security issues in online distance learning. *Vine, 31*(2), 28–35.

Garg, M., & Goel, A. (2022). A systematic literature review on online assessment security: Current challenges and integrity strategies. *Computers & Security, 113,* 102544. . https://doi.org/10.1016/j.cose.2021. 102544

George, D., & Mallery, M. (2003). *Using SPSS for Windows step by step: A simple guide and reference*. https://doi.org/10.4324/9780429056765

Gerald, B. (2018). A brief review of independent, dependent and one sample t-test. *International Journal of Applied Mathematics and Theoretical Physics, 4*(2), 50-54.

Graham, J. W. (2009). Missing data analysis: Making it work in the real world. *Annual Review of Psychology, 60,* 549-576. PMID: 18652544.

Guerrero-Dib, J. G., Portales, L., & Heredia-Escorza, Y. (2020). Impact of academic integrity on workplace ethical behavior. *International Journal for Educational Integrity, 16*(1), 1-18.

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *52*(2), 25-67.

Hale, J. L., Householder, B. J., & Greene, K. L. (2002). The theory of reasoned action. *The persuasion handbook: Developments in Theory and Practice*, *14*(2002), 259-286.

Halim, A., Vandhini, I. S., Saputra, H., & Herliana, F. (2021, September). Acceptance of e-learning media in quantum physics learning based on the TAM model. In 2nd *International Conference on Science, Technology, and Modern Society (ICSTMS 2020)* (pp. 357-361). Atlantis Press.

Hamutoglu, N. B., Gemikonakli, O., Duman, I., Kirksekiz, A., & Kiyici, M. (2020). Evaluating students’ experiences using a virtual learning environment: Satisfaction and preferences. *Educational Technology Research and Development, 68*(1), 437-462.

He, J., & Freeman, L. A. (2010). Are men more technology-oriented than women? The role of gender on the development of general computer self-efficacy of college students. *Journal of Information Systems Education*, *21*(2), 203-212.

Huda, S. S. M., Kabir, M., & Siddiq, T. (2020). E-assessment in higher education: students' perspective. *International Journal of Education and Development using Information and Communication Technology, 16*(2), 250-258.

Husain, T., & Budiyantara, A. (2020). Analysis of control security and privacy based on e-learning users. *SAR Journal, 3*(2), 51-58.

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). A study on cybersecurity challenges in e-learning and database management system. In *Proceedings of the 2020 8th International Symposium on Digital Forensics and Security*, (pp. 1-5). IEEE.

Ibrahim, R., Leng, N. S., Yusoff, R. C. M., Samy, G. N., Masrom, S., & Rizman, Z. I. (2017). E-learning acceptance based on technology acceptance model (TAM). *Journal of Fundamental and Applied Sciences, 9*(4S), 871-889.

Ige, O. A. (2020). School-based cybersecurity education program for schoolchildren in South Africa: A timely call from Bloemfontein. *Universal Journal of Educational Research, 8*(6), 2710-2716.

Ismael, H. R., & Ameen, S. Y. (2022, March). Investigation and development of transparent online assessment: A case study at DPU. In *2022 International Conference on Decision Aid Sciences and Applications* (DASA) (pp. 66-70). IEEE.

Islam, M., Rahim, N. A. A., Liang, T. C., & Momtaz, H. (2011). Effect of demographic factors on e-learning effectiveness in a higher learning Institution in Malaysia. *International Education Studies, 4*(1), 112-121.

Işman, A., & Çelikli, G. E. (2009). How does student ability and self-efficacy affect the usage of computer technology. *The Turkish Online Journal of Educational Technology*, 8(1), 33–38.

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud?. *Journal of Information Technology & Politics*, *5*(3), 269-283.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology, 1*(2), 7-9.

Johnson, D. G. (1985). *Computer ethics*. Englewood Cliffs: Prentice Hall.

Johnson, S. M., & Davis, M. L. (2022). Comparative analysis of linear regression and multiple regression models for predictive modeling. *Journal of Statistical Methods, 47*(3), 123-140. https://doi.org/10.1080/12345678.2022.123456

Jones, S. (2002). *The Internet goes to college: How students are living in the future with today's technology*. Pew Internet & American Life Project.

Kacurova, M., Stevanoski, G., & Bogatinov, D. (2021). Security and privacy with e-learning software. *Етима, 1*(1), 164-173.

Kaiiali, M., Ozkaya, A., Altun, H., Haddad, H., & Alier, M. (2016). Designing a secure exam management system (SEMS) for M-learning environments. *IEEE Transactions on Learning Technologies, 9*(3), 258-271.

Kaminski, J. (2011). Diffusion of innovation theory. *Canadian Journal of Nursing Informatics, 6*(2), 1-6.

Kanimozhi, S., Kannan, A., Suganya Devi, K., & Selvamani, K. (2019). Secure cloud-based e-learning system with access control and group key mechanism. *Concurrency and Computation: Practice and Experience, 31*(12), e4841.

Khalaf, M., M Abdel Azim, Z., HAH Elkhateeb, W., & R Shahin, O. (2022). Explore the e-learning management system lower usage during COVID-19 pandemic. *Information Sciences Letters, 11*(2), 53.

Khan, F., & Alotaibi, R. (2020). Design and implementation of a computerized user authentication system for e-Learning. *International Journal of Emerging Technologies in learning, 15*(9), 4-18.

Khdour, T. (2020). A semantic assessment framework for e-learning systems. *International Journal of Knowledge and Learning, 13*(2), 110-122.

Khlifi, Y. (2020). An advanced authentication scheme for e-evaluation using students behaviors over e-learning platform. *International Journal of Emerging Technologies in Learning*, *15*(4).

Khlifi, Y., & El-Sabagh, H. A. (2017). A novel authentication scheme for e-assessments based on student behavior over e-learning platform. *International Journal of Emerging Technologies in Learning, 12*(4), 62-89.

Khorrami-Arani, O. (2001). Researching computer self-efficacy. *International Education Journal*, *2*(4), 17-25.

Khuluqo, I. E., Ghani, A. R. A., & Fatayan, A. (2021). Postgraduate students' perspective on supporting "learning from home" to solve the COVID-19 pandemic. *International Journal of Evaluation and Research in Education*, *10*(2), 615-623.

Kim, S. S. (2021). Motivators and concerns for real-time online classes: Focused on the security and privacy issues. *Interactive Learning Environments, 31*(4), 1875-1888.

Kim, H. Y. (2013). Statistical notes for clinical researchers: Assessing normal distribution (2) using skewness and kurtosis. *Restorative Dentistry & Endodontics*, *38*(1), 52-54.

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection, 25*, 36-49.

Kong, L., Chu, Z., & Li, Y. (2021). A study of effects of e-learning based exploratory education on students' self-efficacy and interpersonal relationship. *Revista de Cercetare si Interventie Sociala, 72*, 33-43. DOI: 10.33788/ rcis.72.2.

Kotsilieris, T., & Dimopoulou, N. (2013). The evolution of e-learning in the context of 3d virtual worlds. *Electronic Journal of E-Learning*, *11*(2), 147-167.

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review, 33*, 1-48. https://doi.org/10.1016/J.COSREV.2019.05.002

Kumar, P., & Tandon, U. (2022). Factors impacting educators' intention towards e-learning adoption. *ECS Transactions*, *107*(1), 6561.

Kwon, K., Ottenbreit-Leftwich, A. T., Sari, A. R., Khlaif, Z., Zhu, M., Nadir, H., & Gok, F. (2019). Teachers' self-efficacy matters: Exploring the integration of mobile computing device in middle schools. *TechTrends*, *63*(6), 682-692.

Land, K. C. (1969). Principles of path analysis. *Sociological Methodology*, *1*, 3-37.

Langenfeld, T. (2020). Internet-based proctored assessment: Security and fairness issues. *Educational Measurement: Issues and Practice, 39*(3), 24-27.

Lara, J. A., Aljawarneh, S., & Pamplona, S. (2020). Special issue on the current trends in e-learning assessment. *Journal of Computing in Higher Education, 32*(1), 1-8.

Lederman, D., Harrison, D., Fisher Jr, M. R., & Bandy, J. (2020). Best way to stop cheating in online courses?'Teach better'. *Inside Higher Ed.*

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems, 12*(1), 50.

Lee, S., & Lee, D. K. (2018). What is the proper way to apply the multiple comparison test?. *Korean Journal of Anesthesiology*, *71*(5), 353-360.

Lee, B. C., Yoon, J. O., & Lee, I. (2009). Learners' acceptance of e-learning in South Korea: Theories and results. *Computers & education*, *53*(4), 1320-1329.

Leedy, P. D., & Ormrod, J. E. (2019). Practical research: Planning and design. Pearson. One Lake Street, Upper Saddle River, New Jersey 07458.

Levin, K. A. (2006). Study design III: Cross-sectional studies. *Evidence-based dentistry, 7*(1), 24-25.

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for industry 4.0 in the current literature: A reference framework. *Computers in Industry, 103*, 97-110.

Li, J. (2021). Cybercrime in the Philippines: A case study of national security. *Turkish Journal of Computer and Mathematics Education*, *12*(11), 4224-4231.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Little, R. J., & Rubin, D. B. (2019). *Statistical analysis with missing data* (Vol. 793). John Wiley & Sons.

Livingston, E. H. (2004). Who was student and why do we care so much about his t-test? 1. *Journal of Surgical Research*, *118*(1), 58-65.

Longo, F., Padovano, A., & Umbrello, S. (2020). Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future. *Applied Sciences*, *10*(12), 4182.

Lumley, T., Diehr, P., Emerson, S., & Chen, L. (2002). The importance of the normality assumption in large public health data sets. *Annual review of public health*, *23*(1), 151-169.

Lundblad, J. P. (2003). A review and critique of Rogers' diffusion of innovation theory as it applies to organizations. *Organization Development Journal*, *21*(4), 50.

Luppicini, R., & Walabe, E. (2021). Exploring the socio-cultural aspects of e-learning delivery in Saudi Arabia. *Journal of Information, Communication and Ethics in Society.*

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.

Macfarlane, B., Zhang, J., & Pun, A. (2014). Academic integrity: A review of the literature. *Studies in Higher Education, 39*(2), 339-358.

Maharani, M. R., & Usman, O. (2021). The effect of perceived usefulness and perceived ease of use on the use of e-learning with TAM model in faculty of economics student of Jakarta State University. *Jurnal Pendidikan Ekonomi, Perkantoran, Dan Akuntansi, 2*(3), 427-438.

Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytech. Hung, 18,* 67-89.

Mailizar, M., Burg, D., & Maulina, S. (2021). Examining university students' behavioral intention to use e-learning during the COVID-19 pandemic: An extended TAM model. *Education and Information Technologies, 26*(6), 7057-7077.

Mailizar, M., Almanthari, A., & Maulina, S. (2021). Examining teachers' behavioral intention to use e-learning in teaching of mathematics: An extended TAM model. *Contemporary Educational Technology, 13*(2), ep298.

Makarova, M. (2019). Factors of academic misconduct in a cross-cultural perspective and the role of integrity systems. *Journal of Academic Ethics, 17*(1), 51-71.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). Privacy sharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security, 88,* 101653.

Malanga, A. C. M., Bernardes, R. C., Borini, F. M., Pereira, R. M., & Rossetto, D. E. (2022). Towards integrating quality in theoretical models of acceptance: An extended proposed model applied to e-learning services. *British Journal of Educational Technology, 53*(1), 8-22.

Malik, N., Nanda, P., Arora, A., He, X., & Puthal, D. (2018, August). Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 674-679). IEEE.

Malli, A. Y., Ekinci, H. B., Seçer, E., Demirel, N., & Şam, C. T. (2021). Investigation of readiness and expectations of students of sports science faculties regarding the e-learning process and their self-efficacy perceptions.

Mardon, A., Barara, G., Chana, I., Di Martino, A., Falade, I., Harun, R., ... & Varghese, N. (2021). Cryptography.

Martínez-Mesa, J., González-Chica, D. A., Bastos, J. L., Bonamigo, R. R., & Duquia, R. P. (2014). Sample size: How many participants do I need in my research? *Anais brasileiros de dermatologia*, *89*(4), 609–615. https://doi.org/10.1590/abd1806-4841.20143705

Manstead, A. S. R. (2011). The benefits of a critical stance: A reflection on past papers on the theories of reasoned action and planned behaviour. *British Journal of Social Psychology, 50*(3), 366-373.

Mapuva, J. (2009). Confronting challenges to e-learning in higher education institutions. *International Journal of Education and Development Using ICT, 5*(3), 101-114.

McCallister, E. (2010). *Guide to protecting the confidentiality of personally identifiable information* (Vol. 800, No. 122). Diane Publishing.

Meinhardt-Injac, B., & Skowronek, C. (2022). Computer self-efficacy and computer anxiety in social work students: Implications for social work education. *Nordic Social Work Research*, 1-14.

Melissa Ng Lee Yen, A. (2020). The influence of self-regulation processes on metacognition in a virtual learning environment. *Educational Studies, 46*(1), 1-17.

Mellar, H., Peytcheva-Forsyth, R., Kocdar, S., Karadeniz, A., & Yovkova, B. (2018). Addressing cheating in e-assessment using student authentication and authorship checking systems: teachers' perspectives. *International Journal for Educational Integrity, 14*(1), 2.

Mertler, C. A., & Vannatta, R. A. (2016). *Advanced and multivariate statistical methods: Practical application and interpretation*. Taylor & Francis.

Mick, D. G. (1996). Are studies of dark side variables confounded by socially desirable responding? The case of materialism. *Journal of Consumer Research*, *23*(2), 106-119.

Modiba, N., Ojo, S., & Ncube, Z. (2019, October). An ontology-based model for cyber security awareness education. In *ICICIS* (pp. 169-179).

Mohamad, M. A., Amron, M. T., & Noh, N. H. M. (2021, December). Assessing the acceptance of e-learning via technology acceptance model (TAM). In *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering* (Vol. 6, pp. 1-5). IEEE.

Mohammed, H. M., & Ali, Q. I. (2022). E-proctoring systems: A review on designing techniques, features and abilities against threats and attacks. *Quantum Journal of Engineering, Science And Technology, 3*(2), 14-30.

Montano, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health behavior: Theory, Research and Practice*, *70*(4), 231.

Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*, *115*, 619-640.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behavior in improving cyber security management. *Frontiers in Psychology*, 12.

Mukumba, P., & Shambira, N. (2022). Students' technology preference and computer technology applications in the teaching and learning of physics modules at the university undergraduate level in South Africa during the COVID-19 pandemic. *Education Sciences*, *12*(11), 771.

Mungania, P. (2003). Seven e-learning barriers facing employees: Executive summary of dissertation. University of Louisville, (Online). https://www.masie.com/researchgrants/2003/mungania_exec_summary.pdf.

Mystakidis, S., Berki, E., & Valtanen, J. P. (2021). Deep and meaningful e-learning with social virtual reality environments in higher education: A systematic literature review. *Applied Sciences*, *11(*5), 2412.

Nachar, N. (2008). The Mann-Whitney U: A test for assessing whether two independent samples come from the same distribution. *Tutorials in Quantitative Methods for Psychology*, *4*(1), 13-20.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). *Blockchain for secure ehrs sharing of mobile cloud based e-health systems*. IEEE.

Nissa, P. K., & Dheanti, B. L. (2021). The e-learning design for problem based learning in dynamic fluid topic using microsoft sway. *Jurnal Penelitian & Pengembangan Pendidikan Fisika*, *7*(2), 115-122.

Nunnally, J. C., & Bernstein, I. (1994). The assessment of reliability. *Psychometric theory* (3rd ed., pp. 248-292). McGraw-Hill.

Nyoro, M., Kamau, J. W., Wanyembi, G. W., Titus, W. S., & Dinda, W. A. (2015). Review of technology acceptance model usage in predicting e-commerce adoption. *International Journal of Application or Innovation in Engineering & Management, 4*(1), 46-49.

Oetomo, B. S. D., & Santoso, S. (2022). The influences of the learner's ability and the information technology on the learning effectiveness in the e-learning era. *International Journal of Information, Business and Management, 14*(2), 128-139.

Okada, A., Noguera, I., Alexieva, L., Rozeva, A., Kocdar, S., Brouns, F., Ladonlahti, T., Whitelock, D., & Guerrero-Roldán, A. (2019). Pedagogical approaches for e-assessment with authentication and authorship verification in Higher Education. *British Journal of Educational Technology. 50,* (3264–3282).

Okuonghae, O., Igbinovia, M. O., & Adebayo, J. O. (2022). Technological readiness and computer self-efficacy as predictors of e-learning adoption by LIS students in Nigeria. *Libri, 72*(1), 13-25.

Orcan, F. (2020). Parametric or non-parametric: Skewness to test normality for mean comparison. *International Journal of Assessment Tools in Education*, *7*(2), 255-265.

Oxford University Press (2014). *Oxford online dictionary.* http://www.oxforddictionaries.com/definition/english/Cybersecurity.

Page, R., & Satake, E. (2017). Beyond P values and hypothesis testing: Using the minimum Bayes factor to teach statistical inference in undergraduate introductory statistics courses. *Journal of Education and Learning*, *6*(4), 254-266.

Paraskeva, F., Bouta, H., & Papagianni, A. (2008). Individual characteristics and computer self-efficacy in secondary education teachers to integrate technology in educational practice. *Computers & Education*, *50*(3), 1084-1091.

Paris, B., Reynolds, R., & McGowan, C. (2022). Sins of omission: Critical informatics perspectives on privacy in e-learning systems in higher education. *Journal of the Association for Information Science and Technology, 73*(5), 708-725.

Park, H. S. (2000). Relationships among attitudes and subjective norms: Testing the theory of reasoned action across cultures. *Communication Studies*, *51*(2), 162-175.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management*, *9*(12), 669-710.

Prabha, K. M., & Saraswathi, P. V. (2020). Suppressed k-anonymity multi-factor authentication based schmidt-samoa cryptography for privacy preserved data access in cloud computing. *Computer Communications*, *158*, 85-94.

Prakosa, A., & Sumantika, A. (2021, March). An analysis of online shoppers' acceptance and trust toward electronic marketplace using TAM model. *Journal of Physics: Conference Series* (Vol. 1823, No. 1, p. 012008). IOP Publishing.

Preissner, C. E., Kaushal, N., Charles, K., & Knäuper, B. (2022). A protection motivation theory approach to understanding how fear of falling affects physical activity determinants in older Adults. *Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, *78*(1), 30-39.

Prematunga, R. K. (2012). Correlational analysis. *Australian Critical Care*, *25*(3), 195-199.

Proskura, S. L., & Lytvynova, S. H. (2020). The approaches to web-based education of computer science bachelors in higher education institutions. *CTE Workshop Proceedings*, *7*, 609–625. https://doi.org/10.55056/cte.416

Pyke, A., Rovira, E., Murray, S., Pritts, J., Carp, C. L., & Thomson, R. (2021). Predicting individual differences to cyber-attacks: Knowledge, arousal, emotional and trust responses. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *15*(4). https://doi.org/10.5817/CP2021-4-9

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. *IEEE Internet of Things Journal*, *7*(6), 4682-4696.

Rahmi, B. A. K. I., Birgoren, B., & Aktepe, A. (2018). A meta-analysis of factors affecting perceived usefulness and perceived ease of use in the adoption of e-learning systems. *Turkish Online Journal of Distance Education*, *19*(4), 4-42.

Raj, S., & Nayak, M. M. (2020). Why defensive security should be compulsory subject to internet users. *International Journal of Electrical Engineering and Technology*, *11*(10), 234-239.

Redfern, N. (2015). The log-normal distribution is not an appropriate parametric model for shot length distributions of Hollywood films. *Digital Scholarship in the Humanities*, *30*(1), 137-151.

Rice, J. A. (2006). *Mathematical statistics and data analysis*. Cengage Learning.

Rjaibi, N., & Rabai, L. B. A. (2018). How stakeholders perceived security risks? A new predictive functional level model and its application to e-learning. *EAI Endorsed Transactions on Security and Safety, 5*(15), e3.

Rjaibi, N., Rabai, L. B. A., Aissa, A. B., & Louadi, M. (2012). Cyber security measurement in depth for e-learning systems. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*(11), 107-120.

Rogers, E.M. (1995). Diffusion of innovations. (4th ed.) New York: *The Free Press.*

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2014). Diffusion of innovations. In *D. Stacks (Ed.), An integrated approach to communication theory and research* (pp. 432-448). Routledge.

Rokhman, F., Mukhibad, H., Bagas Hapsoro, B., & Nurkhin, A. (2022). E-learning evaluation during the COVID-19 pandemic era based on the updated of Delone and McLean information systems success model. *Cogent Education*, *9*(1), https://doi.org/ 10.1080/2331186X.2022.2093490.

Romansky, R., & Noninska, I. (2015). Implementation of security and privacy principles in e-learning architecture. In *Proceedings of the International Conference on Information Technologies* (pp. 66-77). St. St. Constantine and Elena, Bulgaria.

Šabić, J., Baranović, B., & Rogošić, S. (2022). Teachers' self-efficacy for using information and communication technology: The interaction effect of gender and age. *Informatics in Education*, *21*(2), 353-373.

Salloum, S. A., Alhamad, A. Q. M., Al-Emran, M., Monem, A. A., & Shaalan, K. (2019). Exploring students’ acceptance of e-learning through the development of a comprehensive technology acceptance model. *IEEE Access*, *7*, 128445-128462. doi: https://doi.org/10.1109/ACCESS.2019.2939467

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8.

Schlebusch, C. L. (2018). Computer anxiety, computer self-efficacy and attitudes towards the internet of first year students at a South African University of Technology. *Africa Education Review*, *15*(3), 72-90.

Seliana, N., Suroso, A. I., & Yuliati, L. N. (2020). Evaluation of e-learning implementation in the university using DeLone and McLean success model. *Jurnal Aplikasi Manajemen*, *18*(2), 345-352.

Senel, S., & Senel, H. C. (2021). Remote assessment in higher education during COVID-19 pandemic. *International Journal of Assessment Tools in Education, 8*(2), 181-199.

Seta, H. B., Wati, T., Muliawati, A., & Hidayanto, A. N. (2018). E-learning success model: An extention of DeLone & McLean IS' success model. *Indonesian Journal of Electrical Engineering and Informatics, 6*(3), 281-291.

Setia, M. S. (2016). Methodology series module 3: Cross-sectional studies. *Indian Journal of Dermatology*, *61*(3), 261.

Shaffer, J. P. (1995). Multiple hypothesis testing. *Annual review of psychology*, *46*(1), 561-584.

Shamir-Inbal, T., & Blau, I. (2021). Characteristics of pedagogical change in integrating digital collaborative learning and their sustainability in a school culture: e-CSAMR framework. *Journal of Computer Assisted Learning*, *37*(3), 825-838.

Sharifov, M., Safikhanova, S., & Mustafa, A. (2021). Review of prevailing trends barriers and future perspectives of learning management systems (lmss) in higher education institutions. *International Journal of Education and Development using Information and Communication Technology*, *17*(3), 207-216.

Shdaifat, S. A. K. (2020). The future role of vocational education teachers in the professional learning communities in public schools from the perspective of principals and academic supervisors in Jordan. *International Journal of Higher Education*, *9*(5), 322-337.

Shdaifat, S. A. K., Shdaifat, N. A., & Khateeb, L. A. (2020). The reality of using e-learning applications in vocational education courses during COVID 19 crisis from the vocational education teachers' perceptive in Jordan. *International Education Studies*, *13*(10), 105-112.

Singh, S. (2006). Cultural differences in, and influences on, consumers’ propensity to adopt innovations. *International Marketing Review*, *23*(2), 173-191.

Singh, M., Adebayo, S. O., Saini, M., & Singh, J. (2021). Indian government e-learning initiatives in response to COVID-19 crisis: A case study on online learning in Indian higher education system. *Education and Information Technologies*, *26*(6), 7569-7607.

Sloan, R., & Warner, R. (2017). *Unauthorized access: The crisis in online privacy and security*. Taylor & Francis.

Smith, J. D., & Johnson, A. R. (2022). Exploring the differences between linear regression and multiple regression: A Comparative study. *Journal of Statistical Analysis, 28*(3), 45-62. https://doi.org/10.1080/12345678.2022.123456

Smith, J., Johnson, A., & Brown, L. (2022). Assessing the normality of data distributions using histograms with Normal Curve. *Journal of Research Methods, 14*(3), 201-216.

Smith, J., Johnson, A., & Lee, K. (2023). Data preprocessing hygiene: Best practices for ensuring data quality in machine learning. *Journal of Data Science, 7*(2), 45-62.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178-188.

Stratton, S. J. (2021). Population research: convenience sampling strategies. *Prehospital and Disaster Medicine*, *36*(4), 373-374.

Suhr, D. (2006). Exploratory or confirmatory factor analysis? In *SAS Users Group International Conference* (pp. 1-17). SAS Institute, Inc.

Sulaymani, O., Pratama, A. R., Alshaikh, M., & Alammary, A. (2022). The effects of previous experience and self efficacy on the acceptance of e-learning platforms among younger students in Saudi Arabia. *Contemporary Educational Technology*, *14*(2), ep349.

Sundeen, T. H., & Kalos, M. (2022). Rural educational leader perceptions of online learning for students with and without disabilities before and during the COVID-19 pandemic. *Theory & Practice in Rural Education*, *12*(2), 105-128.

Sun, Z. (2019). A study on the educational use of statistical package for the social sciences. *International Journal of Frontiers in Engineering Technology*, *1*(1), 20-29.

Swanson, M., & Guttman, B. (1996). *Generally accepted principles and practices for securing information technology systems*. National Institute of Standards and Technology, Technology Administration, US Department of Commerce.

Tabachnick, B. G., Fidell, L.S. and Ullman, J. B. (2007). *Using multivariate statistics*. Pearson.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493-9532.

Tabsh, S. W., El Kadi, H. A., & Abdelfatah, A. S. (2019, April). Faculty perception of engineering student cheating and effective measures to curb it. In *2019 IEEE Global Engineering Education Conference (EDUCON)* (pp. 806-810). IEEE.

Taha, N., & Dahabiyeh, L. (2021). College students' information security awareness: A comparison between smartphones and computers. *Education and Information Technologies*, *26(*2), 1721-1736.

Taherdoost, H. A. M. E. D., Sahibuddin, S., & Jalaliyoon, N. E. D. A. (2022). Exploratory factor analysis: Concepts and theory. *Advances in Applied and Pure Mathematics*, *27*, 375-382.

Talosa, A. D., Javier, B. S., & Dirain, E. L. (2021). The flexible-learning journey: Phenomenological investigation of self-efficacy influencing factors among higher education students. *Linguistics and Culture Review*, *5*(S3), 422-434.

Tao, X., Liu, Y., Wong, P. K. Y., Chen, K., Das, M., & Cheng, J. C. (2022). Confidentiality-minded framework for blockchain-based BIM design collaboration. *Automation in Construction*, *136*, 104172. 10.1016/j.autcon.2022.104172

Tawafak, R. M., Romli, A., Malik, S. I., & Alfarsi, G. (2021, May). Integration of TAM and MOOC for e-learning purpose. In *AIP Conference Proceedings* (Vol. 2339, p. 020056). AIP Publishing LLC.

Thowfeek, M. H., & Jaafar, A. (2012). Instructors' view about implementation of e-learning system: An analysis based on hofstede's cultural dimensions. *Procedia-Social and Behavioral Sciences*, *65*(2012), 961-967.

Tick, A. (2018, June). IT security as a special awareness at the analysis of the digital/e-learning acceptance strategies of the early z generation. In *2018 IEEE 22nd International Conference on Intelligent Engineering Systems.* (pp. 45-50). IEEE.

Tirumala, S. S., & Shahamiri, S. R. (2016, November). A review on deep learning approaches in speaker identification. In *Proceedings of the 8th international conference on signal processing systems* (pp. 142-147).

To, A. T., & Trinh, T. H. M. (2021). Understanding behavioral intention to use mobile wallets in vietnam: Extending the tam model with trust and enjoyment. *Cogent Business & Management, 8*(1), 1891661.

Tomczyk, Ł., & Walker, C. (2021). The emergency (crisis) e-learning as a challenge for teachers in Poland. *Education and Information Technologies, 26*(6), 6847-6877.

Trim, P. R., & Lee, Y. I. (2021). The global cyber security model: Counteracting cyber-attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing, 5*(3), 32.

Turnbull, D., Chugh, R., & Luck, J. (2021). Transitioning to e-learning during the COVID-19 pandemic: How have higher education institutions responded to the challenge? *Education and Information Technologies*, 1-19.

Udroiu, A. M. (2018). Implementing the cybersecurity awareness program using e-learning platform. In *Conference Proceedings of eLearning and Software for Education «(eLSE)* (Vol. 14, No. 04, pp. 101-104). Carol I National Defence University Publishing House.

Udin, T., Maufur, S., & Riyanto, O. R. (2022). Student's self-efficacy and perceptions of online learning on the use learning management system. *Journal of Education Technology, 6*(1).

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39.

Upadhyay, D., & Sampalli, S. (2020). SCADA (supervisory control and data acquisition) systems: vulnerability assessment and security recommendations. *Computers & Security, 89,* 101666.

Ursachi, G., Horodnic, I. A., & Zait, A. (2015). How reliable are measurement scales? External factors with indirect influence on reliability estimators. *Procedia Economics and Finance, 20*, 679–686. https://doi.org/10.1016/s2212-5671(15)00123-9

Vaswani, N. (2021). Cyber-attacks: An economic impact. *Supremo Amicus, 23*, 297.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342-365.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273-315.

Venkatesh, V., & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. MIS Quarterly, 24(1), 115-139. http://dx.doi.org/10.2307/3250981

Venkatesh, V., Morris, M. G., & Ackerman, P. L. (2000). A longitudinal field investigation of gender differences in individual technology adoption decision-making processes. *Organizational Behavior and Human Decision Processes, 83*(4), 33-60. http://dx.doi.org/10.1006/obhd.2000.2896

Wahid, S. D. M. (2021). Cyber security behaviorin online distance learning: Utilizing national e-learning policy. *Turkish Journal of Computer and Mathematics Education, 12*(5), 1719-1728.

Wakunuma, K., & Masika, R. (2017). Cloud computing, capabilities and intercultural ethics: Implications for Africa. *Telecommunications Policy*, *41*(695-707).

Westcott, R., Ronan, K., Bambrick, H., & Taylor, M. (2017). Expanding protection motivation theory: Investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychology, 5*(1), 1-14.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM*, *46*(8), 91-95.

Wiley. (2020). *Academic integrity in the age of online learning: Survey shows sharp rise in instructor perception of cheating*. https://www.wiley.com/network/instructors-students/covid-19-onlineteaching-resources-1/is-student-cheating-on-the-rise-how-you-can-discourage-it-in-your-classroom

Williams, C. (2007). Research methods. *Journal of Business & Economics Research*, *5*(3), 65-71.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816.

World Health Organization. (2020). *World health organization coronavirus disease (COVID-19) dashboard.* https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public.

Wu, Z., Xuan, S., Xie, J., Lin, C., & Lu, C. (2022). How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. *Computers in Biology and Medicine*, *147*, 105726.

Yang, B. (2005). Factor analysis methods. *Research in organizations: Foundations and Methods of Inquiry*, (pp. 181-199). Berrett-Koehler.

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723-131740.

Yong, A. G., & Pearce, S. (2013). A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in Quantitative Methods for Psychology*, *9*(2), 79-94.

You, W. (2022). Research on the relationship between learning engagement and learning completion of online learning students. *International Journal of Emerging Technologies in Learning*, *17*(1), 102-117.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, *16*(4), 490-513.

Yusuf, R. A., & Awoyemi, O. O. (2022). Cyber security and its implication on library users'privacy. *Owena Journal Of Library And Information Science*, *9*(1).

Zhang, Y., & Espinoza, S. (1998). Relationships among computer self-efficacy, attitudes toward computers, and desirability of learning computing skills. *Journal of Research on Computing in Education*, *30*(4), 420-436.

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys*, *54*(1), 1-39.

Zhao, G., Rong, C., Li, J., Zhang, F., & Tang, Y. (2010, November). Trusted data sharing over untrusted cloud storage providers. In *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (pp. 97-103). IEEE Computer Society.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.

APPENDICES

Appendix A: Consent Form & Survey Questions

Towards Sustainable E-Learning Platforms in the Context of Cybersecurity: A TAM-Driven Approach

Hebah Alquran
Eastern Michigan University- Game above College of Engineering and Technology

This survey conducted by Hebah Alquran as part of a PhD dissertation at Eastern Michigan University. The purpose of this survey is to obtain your perceptions toward adopting e-learning platforms when registering for your upcoming courses next semesters or in future according to the factors of Cybersecurity perspectives, Privacy Concerns, Cybersecurity Awareness, Academic Integrity (AI) Concerns, and Computer Self-Efficacy (CSE). The information that you provide will remain completely confidential. Your identity will remain completely anonymous.

Dear Student,

As a Ph. D. Candidate at Eastern Michigan University (EMU), I am conducting research for my dissertation that will investigate the factors that affect graduate and undergraduate students' intention to use e-learning platforms at EMU within cybersecurity context. For this purpose, I have created a questionnaire to be used in an anonymous Web-based survey. This instrument is designed to get a better understanding about issues that influence students' intention to register for classes online. The survey will help in assessing the factors that predict the intension to use the e-learning platforms. The findings will contribute to the broader research on use of information technology in e-learning platforms.

Whether or not you currently use e-learning platforms for your instruction, your participation in this study is extremely important. I would appreciate you taking the time (approximately 15-20 minutes) to complete and submit this online survey by **February 28, 2023.**

Before participating in the survey, please read the study information below. This informs you of your rights as a research participant. If you have any questions, please feel free to contact me by e-mail or phone number that listed below. For more information about your rights as a participant in research, you can contact the Eastern Michigan University Office of Research Compliance at 734-487-3090 or human.subjects@emich.edu.

The survey questions are about your perception towards e-learning systems. Therefore, there is no right or wrong answer. Please, respond to the questions by choosing the answer that best represents your perception about the item.

Sincerely,

Hebah Alquran

PhD. Candidate and Adjunct at EMU

Information Security and Applied Computing (ISAC)
Phone: (734)-757-3391
E-mail: halquran@emich.edu

Informed Consent Form

Description of the Study

The purpose of this survey is to obtain your perceptions toward adopting e-learning platforms when registering for your upcoming courses next semesters or in future according to the factors of Cybersecurity, Cybersecurity Awareness, Privacy, Academic Integrity, and Computer Self-Efficacy. The information that you provide will remain completely confidential. Your identity will remain completely anonymous.

Risks/Benefits

There are currently no anticipated risks associated with this study. By participating in this research, you will contribute to a deeper comprehension of the factors influencing students' inclination to utilize e-learning platforms. This study aims to enhance students' understanding in this area.

Costs and Payments

There are no costs or payments for your participation in this study.

Confidentiality and Privacy

As a participant in this research, the researcher wants to assure you that your anonymity will be safeguarded. Your responses will be included in a database without any identifiable information, ensuring your privacy. All data collected in this study is anonymous, and your individual responses will be treated with strict confidentiality.

Right to Withdraw from the Study

You have the right to decline participation in this survey or choose not to answer any question that makes you uncomfortable. At any point, you are free to discontinue your involvement in the survey.

Storing study information for future use

To ensure privacy and security, your information will be stored for future study purposes. It will be assigned a unique code rather than your name for identification. The data will be securely stored in a password-protected or locked file. It will be retained indefinitely. Specifically, your data will be stored in a password-protected EMU Google Drive, which can only be accessed using EMU credentials.

The laptop utilized for opening, analyzing, and working with the collected data is personally owned by the researcher (myself). Access to the data will be limited to the researcher (myself) and/or my advisor (Dr. Bilquis Ferdousi) solely if she requests it. This ensures restricted access and maintains confidentiality.

Your information may be shared with other researchers without seeking your explicit permission; however, the shared information will always be de-identified and stripped of any identifying details. If requested, we may send your de-identified information via email. Rest assured that any shared data will never include information that could personally identify you.

Voluntary Consent

Participating in this study is entirely voluntary, and you are not obligated to take part in any way. However, by completing and submitting the web-based survey, you indicate your voluntary agreement to participate in this study.

Survey Questions

Please Check the answer which best describes you below.

Variable	**Description**
Gender	□ Man □ Woman □ Transgender/Trans woman □ Transgender/Trans man □ Genderqueer/Non-Binary □ Not Listed: - …………………. □ Prefer not to reply.
Ethnicity	□ Hispanic □ Asian □ Native-American □ Arab □ African American □ Caucasian □ Not Listed: - ………………….
Subject/Discipline	□Technology-Related Major □ Non-Technology Related Major
Level of Education	□ Undergraduate □ Graduate

Please Check the answer which best represent your perspective below.

Cybersecurity Perspectives

The following is a list of statements related to your intended use of e-learning systems in your college. Please read each item and rate the level of likelihood you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly agree'.

#	**Item / Question**	Strongly disagree **1**	Disagree **2**	Neither agree nor disagree **(3)**	Agree **4**	Strongly agree **5**	**ref**

CST1	E-learning platform has a high security policy to protect students’ sensitive information.	Husain & Budiyantara (2020)
CST2	E-learning platform is a secure place where I can share my sensitive information securely.	Husain & Budiyantara (2020)
CST3	E-learning platform is reliable/ confidential.	Husain & Budiyantara (2020)
CST4	E-learning platform provides a multi-factor authentication (e.g. phone number, password, PIN, SMS using smartphones, fingerprint) which makes me feel secure when logging into my account.	Dasgupta et al. (2017)
CST5	The grades obtained from e-exams or online exam in E-learning platform are valid and reliable the same as paper-based exams.	Hillier (2014)
CST6	E-exams or online exams in E-learning platform are fairer than paper-based exams.	Hillier (2014)
CST7	Setting an automated timer for the whole e-exam or each question makes e-exams or online exams more secure than paper-based exams.	Hillier (2014) & Khan et al. (2021)
CST8	The technology used in online exams is sufficiently effective in dealing with cheating and plagiarism.	Khan et al. (2021)

Privacy Concerns

#	Item / Question	**Strongly disagree 1**	Disagree2	Neither agree nor disagree 3	Agree 4	Strongly Agree 5	**Ref**
PV1	In the E-learning platform, I feel uncomfortable to provide my ideas or answers for the threaded discussion assignments.						Chang (2021)
PV2	In the E-learning platform my intellectual property (i.e., assignment works) is not protected.						Maatuk et al. (2022)
PV3	In the online learning platform, I feel uncomfortable in case the instructors record synchronous class meetings (i.e., Zoom meetings) without my permission.						Langenfeld (2020)
PV4	In the E-learning platform, I feel uncomfortable during the proctored online exams because I am being watched and recorded.						Langenfeld (2020)
PV5	The use of my personally identifiable information during the recorded proctored in online exams makes me feel less private.						Langenfeld (2020)
PV6	Storing the recorded video in online exams and sharing them to the host server intercept my privacy.						Langenfeld (2020)
PV7	In the online group-based assignments or projects in E-learning platform, there are less confidential and anonymous peer evaluations which makes the evaluation process unfair and non-reflective to assess their contributions.						(Self-developed) & Tumpa et al. (2022)
PV8	In the E-learning platform, the instructors can detect my logs into the class and know the time I						(Self-developed) &

	spend on the class which makes me uncomfortable.						(Baldwi & Ching, 2019)
PV9	In the E-learning platform, other students can detect and access my personally identifiable information such as my email and profile, which makes me feel unsecure.						Author (Self-developed)
PV10	In the E-learning platform, the instructors can detect my logs into the class which makes me feel uncomfortable.						Author (Self-developed)

Cybersecurity Awareness

#	Item / Question	Strongly disagree 1	Disagree 2	Neither agree nor disagree 3	Agree 4	Strongly Agree 5	Ref
CSW1	I feel competent to use of computers.						(Erendor & Yildirim, 2022)
CSW2	I have a good knowledge regarding computer hardware, software, and operating systems.						(Erendor & Yildirim, 2022)
CSW3	I have a good knowledge regarding the cyber-attacks occur over the computer network systems.						(Erendor & Yildirim, 2022)
CSW4	I have a good knowledge regarding the concept of computer security measures such as HTTPS, secure connection, SSH, and TSL.						(Erendor & Yildirim, 2022)
CSW5	I have a sufficient knowledge regarding the concept of “Cyber						(Erendor &

	Attacks”.	Yildirim, 2022)
CSW6	I know the difference between “Social Engineering” and “Phishing Attacks”.	(Erendor & Yildirim, 2022)
CSW7	The use of my personally identifiable information in e-exams or online exams during the recorded proctoring makes me feel less private.	(Erendor & Yildirim, 2022)

Academic Integrity Concern

#	**Item / Question**	**Strongly disagree 1**	Disagree**2**	Neither agree nor disagree **3**	Agree **4**	Strongly Agree **5**	**Ref**
AI1	In the E-learning platform, many students can share solved assignments easily which makes me feel frustrated.						Wiley (2020); Tomczyk & Walker (2021)
AI2	In the E-learning platform, many students can cheat easily which makes me feel upset.						Wiley (2020); Tomczyk & Walker (2021)
AI3	In the E-learning platform, many students can ask others to take the exam on behave of them which makes me feel unfair.						Wiley (2020); Tomczyk & Walker (2021)
AI4	In the E-learning platform, many students show carelessness in the						Alier et al. (2021)

	online classes which makes me feel less competence.						
AI5	In the E-learning platform, many students don’t comply with attendance, or if attend they turn off their cameras which makes the online learning boring.						Alier et al. (2021)
AI6	In the E-learning platform, many students show less respect to the course which makes me feel uncommitted.						Alier et al. (2021)
AI7	In the E-learning platform, many students show irresponsible behaviors in the course such as playing with their cell phones, chatting, or paly games, which makes me feel unengaged to the course.						Alier et al. (2021)

Computer Self-Efficacy

#	Item / Question	Not Confident at all 1	Less Confident 2	Moderate Confident 3	Confident 4	Totally Confident 5	Ref
CSE1	To use e-learning platforms even if I had never used a system like it before, I would feel						Ferdousi (2009)
CSE2	To use e-learning platforms if someone else helps me get						Ferdousi

	started, I would feel	(2009)
CSE3	To use e-learning platforms if I could call someone for help if I got stuck, I would feel	Ferdousi (2009)
CSE4	To use e-learning platforms if I have just the built-in help facility for assistance, I would feel	Ferdousi (2009)
CSE5	To use e-learning platforms if I have seen someone else using it before trying it myself, I would feel	Ferdousi (2009)
CSE6	To use e-learning platforms if I have only the software manuals for reference, I would feel	Ferdousi (2009)
CSE7	To use e-learning platforms if I have lot of time to complete my instructional job, I will feel	Ferdousi (2009)
CSE8	To use e-learning platforms if no one is around to tell me what to do as I go, I would feel	Ferdousi (2009)
CSE9	To use e-learning platforms if I had used similar systems before this one for instruction, I would feel	Ferdousi (2009)
CSE10	To use e-learning platforms on my own, I would feel	Ferdousi (2009)
CSE11	To download or install e-learning	Ferdou

	software/materials on my own, I would feel						si (2009)
CSE12	To navigate or search for document in any e-learning website, I would feel						Ferdousi (2009)

Intention to use e-learning platforms (ITU)

#	**Item / Question**	**Strongly disagree 1**	**Disagree 2**	**Neither agree nor disagree 3**	**Agree 4**	**Strongly Agree 5**	**Ref**
ITU1	I plan to take my classes offered online asynchronous in future.						Camacho & Legare (2021)
ITU2	I plan to take my classes offered online synchronous in future.						Camacho & Legare (2021)
ITU3	I plan to take my classes offered hybrid in future.	This Item was deleted					Camacho & Legare (2021)
Reverse Coded - ITU4	I plan to take my classes offered in-person in future.						Camacho & Legare (2021)
ITU5	I will encourage others to take classes online.						Farooq et al. (2020)
ITU6	I prefer using the e-						Farooq et al.

	learning platforms than the traditional in-person paper-based method.	(2020)

References for Each Factor

Cybersecurity Perspectives

Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-factor authentication. In Advances in User Authentication (pp. 185-233). *Springer, Cham*.

Hillier, M. (2014, January). The very idea of e-Exams: student (pre) conceptions. *In Proceedings of ASCILITE 2014-Annual Conference of the Australian Society for Computers in Tertiary Education* (pp. 77-88). ascilite.

Husain, T., & Budiyantara, A. (2020). Analysis of Control Security and Privacy Based on e-Learning Users. *SAR Journal, 3*(2), 51-58.

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020, June). A study on cybersecurity challenges in e-learning and database management system. *In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.*

Khan, M. A., Vivek, V., Khojah, M., Nabi, M. K., Paul, M., & Minhaj, S. M. (2021). Learners' perspective towards e-exams during COVID-19 outbreak: Evidence from higher educational institutions of India and Saudi Arabia. *International Journal of Environmental Research and Public Health, 18*(12), 6534.

https://www.elearnmagazine.com/outcomes/multi-factor-authentication-in-your-lms-how-to-enable-it-and-will-it-endanger-you-cybersec-pulse/

Cybersecurity Awareness

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity Awareness in Online Education: A Case Study Analysis. *IEEE Access, 10,* 52319-52335.

Privacy Concerns

Chang, B. (2021). Student privacy issues in online learning environments. *Distance Education, 42*(1), 55-69.

Baldwin, S., & Ching, Y.-H. (2019). Online course design: A review of the canvas course evaluation checklist. *International Review of Research in Open and Distributed Learning, 20*(3), 268–282.

Langenfeld, T. (2020). Internet-based proctored assessment: security and fairness issues. *Educational Measurement: Issues and Practice*, *39*(3), 24-27.

Tumpa, R. J., Skaik, S., Ham, M., & Chaudhry, G. (2022). A holistic overview of studies to improve group-based assessments in higher education: A systematic literature review. *Sustainability*, 14(15), 9638.

CSE

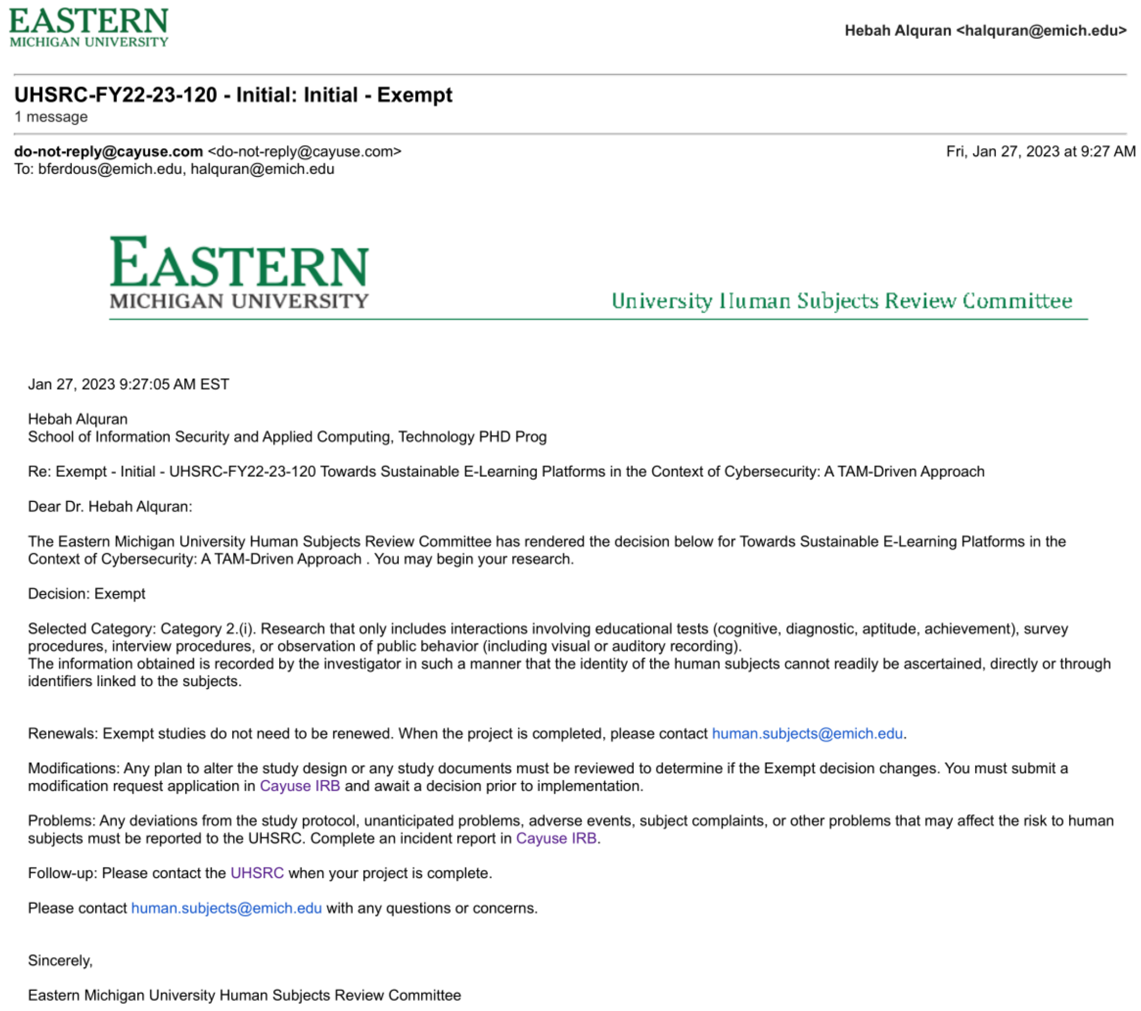
Ferdousi, B. J. (2009). A study of factors that affect instructors' intention to use e-learning systems in two-year colleges. *Nova Southeastern University*.

ITU

Camacho, D. J., & Legare, J. M. (2021). Pivoting to online learning—The future of learning and work. *The Journal of Competency-Based Education*, *6*(1), e1239.

Farooq, A., Ahmad, F., Khadam, N., Lorenz, B., & Isoaho, J. (2020, July). The impact of perceived security on intention to use e-learning among students. In *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)* (pp. 360-364). IEEE.

University Human Subject Review Committee Decision (UHSRC) - Exempt



EASTERN
MICHIGAN UNIVERSITY

Hebah Alquran <halquran@emich.edu>

UHSRC-FY22-23-120 - Initial: Initial - Exempt
1 message

do-not-reply@cayuse.com <do-not-reply@cayuse.com>
To: bferdous@emich.edu, halquran@emich.edu

Fri, Jan 27, 2023 at 9:27 AM

EASTERN
MICHIGAN UNIVERSITY

University Human Subjects Review Committee

Jan 27, 2023 9:27:05 AM EST

Hebah Alquran
School of Information Security and Applied Computing, Technology PHD Prog

Re: Exempt - Initial - UHSRC-FY22-23-120 Towards Sustainable E-Learning Platforms in the Context of Cybersecurity: A TAM-Driven Approach

Dear Dr. Hebah Alquran:

The Eastern Michigan University Human Subjects Review Committee has rendered the decision below for Towards Sustainable E-Learning Platforms in the Context of Cybersecurity: A TAM-Driven Approach . You may begin your research.

Decision: Exempt

Selected Category: Category 2.(i). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording).
The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects.

Renewals: Exempt studies do not need to be renewed. When the project is completed, please contact human.subjects@emich.edu.

Modifications: Any plan to alter the study design or any study documents must be reviewed to determine if the Exempt decision changes. You must submit a modification request application in Cayuse IRB and await a decision prior to implementation.

Problems: Any deviations from the study protocol, unanticipated problems, adverse events, subject complaints, or other problems that may affect the risk to human subjects must be reported to the UHSRC. Complete an incident report in Cayuse IRB.

Follow-up: Please contact the UHSRC when your project is complete.

Please contact human.subjects@emich.edu with any questions or concerns.

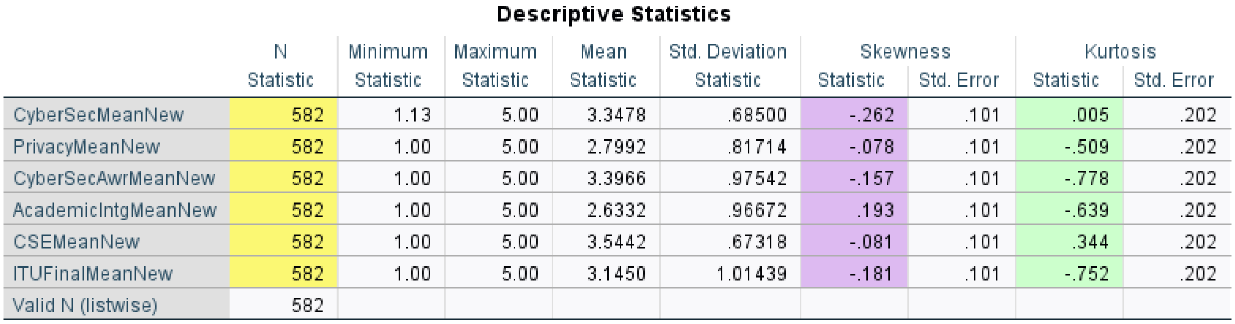
Sincerely,

Eastern Michigan University Human Subjects Review Committee

Appendix B: Part One of Analysis

Table B1

Descriptive Analysis of Computed Variables

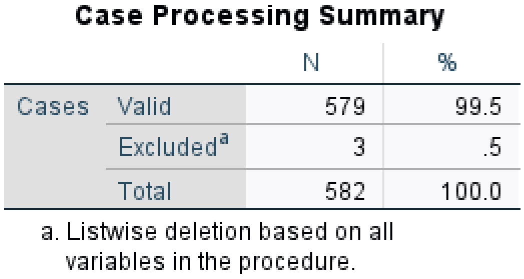


Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
CyberSecMeanNew	582	1.13	5.00	3.3478	.68500	-.262	.101	.005	.202
PrivacyMeanNew	582	1.00	5.00	2.7992	.81714	-.078	.101	-.509	.202
CyberSecAwrMeanNew	582	1.00	5.00	3.3966	.97542	-.157	.101	-.778	.202
AcademicIntgMeanNew	582	1.00	5.00	2.6332	.96672	.193	.101	-.639	.202
CSEMeanNew	582	1.00	5.00	3.5442	.67318	-.081	.101	.344	.202
ITUFinalMeanNew	582	1.00	5.00	3.1450	1.01439	-.181	.101	-.752	.202
Valid N (listwise)	582								

Table B2

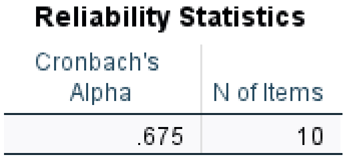
Reliability Test of Cybersecurity Perspectives



Case Processing Summary

		N	%
Cases	Valid	579	99.5
	Excluded[a]	3	.5
	Total	582	100.0

a. Listwise deletion based on all variables in the procedure.

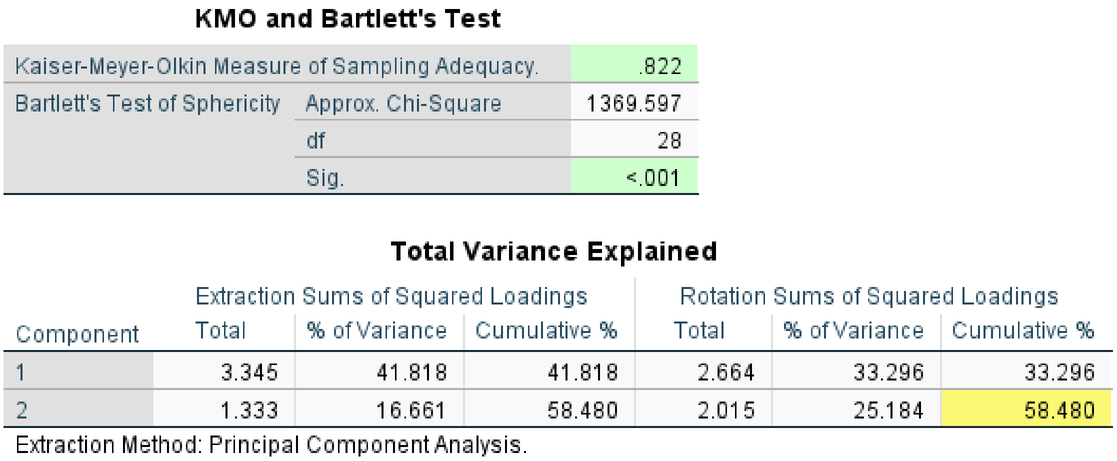


Reliability Statistics

Cronbach's Alpha	N of Items
.675	10

Table B3

KMO for The Eight Items of Cybersecurity Perspectives



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.822
Bartlett's Test of Sphericity	Approx. Chi-Square	1369.597
	df	28
	Sig.	<.001

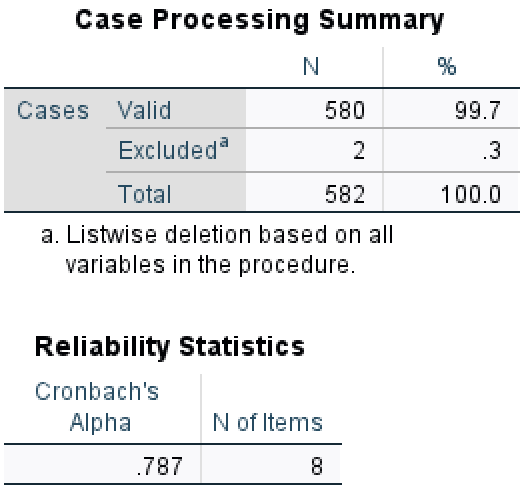
Total Variance Explained

	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.345	41.818	41.818	2.664	33.296	33.296
2	1.333	16.661	58.480	2.015	25.184	58.480

Extraction Method: Principal Component Analysis.

Table B4

Reliability Test for Eight Items of Cybersecurity Perspectives



Case Processing Summary

		N	%
Cases	Valid	580	99.7
	Excluded[a]	2	.3
	Total	582	100.0

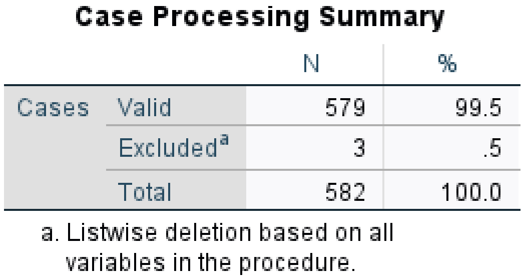
a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.787	8

Table B5

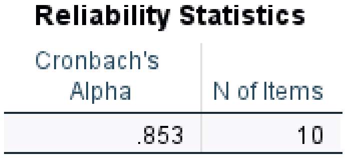
Reliability Test for Items of Privacy Concerns



Case Processing Summary

		N	%
Cases	Valid	579	99.5
	Excluded[a]	3	.5
	Total	582	100.0

a. Listwise deletion based on all variables in the procedure.

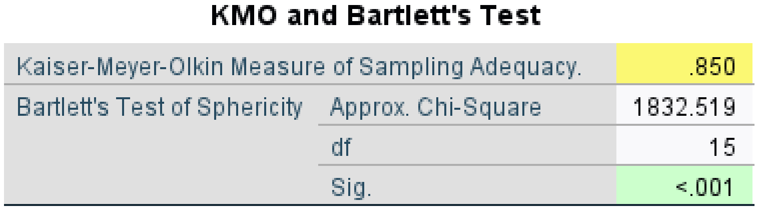


Reliability Statistics

Cronbach's Alpha	N of Items
.853	10

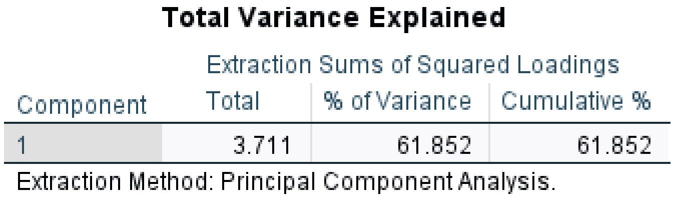
Table B6

KMO of Cybersecurity Awareness



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.850
Bartlett's Test of Sphericity	Approx. Chi-Square	1832.519
	df	15
	Sig.	<.001



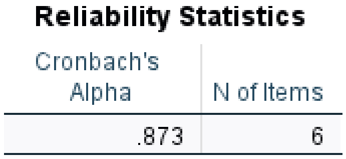
Total Variance Explained

	Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %
1	3.711	61.852	61.852

Extraction Method: Principal Component Analysis.

Table B7

Reliability Test of Cybersecurity Awareness

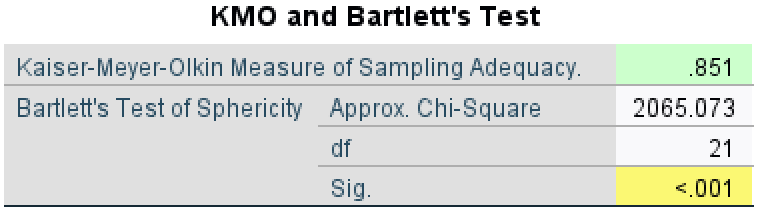


Reliability Statistics

Cronbach's Alpha	N of Items
.873	6

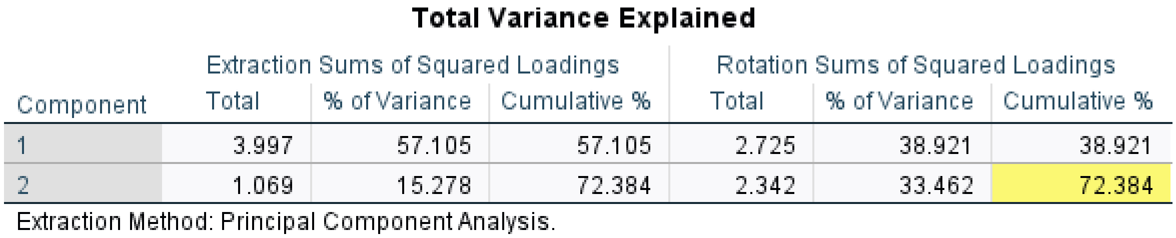
Table B8

KMO of AI Concerns



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.851
Bartlett's Test of Sphericity	Approx. Chi-Square	2065.073
	df	21
	Sig.	<.001



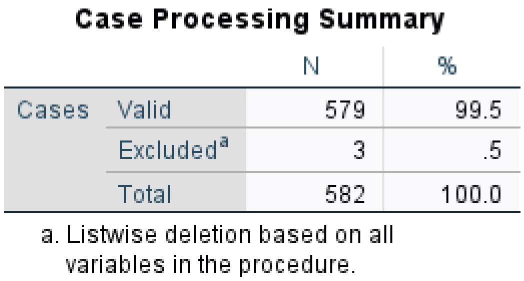
Total Variance Explained

	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.997	57.105	57.105	2.725	38.921	38.921
2	1.069	15.278	72.384	2.342	33.462	72.384

Extraction Method: Principal Component Analysis.

Table B9

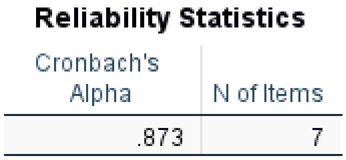
Reliability Analysis of AI Concerns



Case Processing Summary

		N	%
Cases	Valid	579	99.5
	Excluded[a]	3	.5
	Total	582	100.0

a. Listwise deletion based on all variables in the procedure.

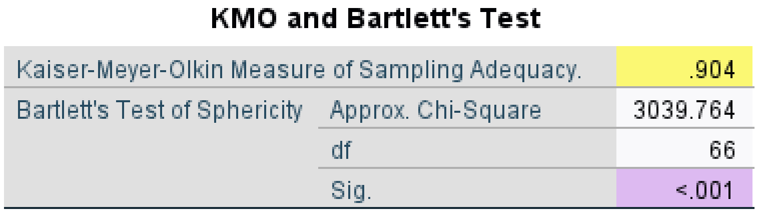


Reliability Statistics

Cronbach's Alpha	N of Items
.873	7

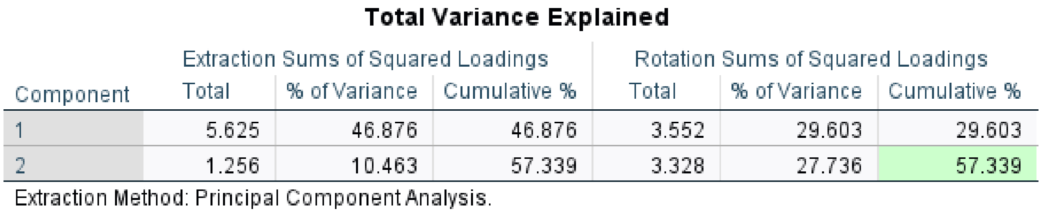
Table B10

Factor Analysis-KMO of CSE



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.904
Bartlett's Test of Sphericity	Approx. Chi-Square	3039.764
	df	66
	Sig.	<.001



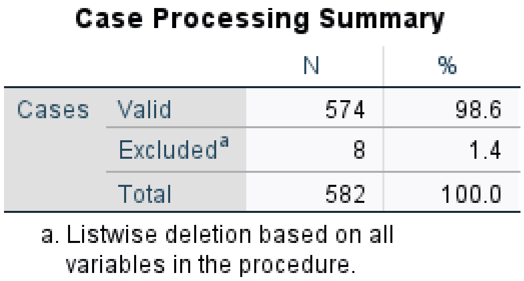
Total Variance Explained

	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.625	46.876	46.876	3.552	29.603	29.603
2	1.256	10.463	57.339	3.328	27.736	57.339

Extraction Method: Principal Component Analysis.

Table B11

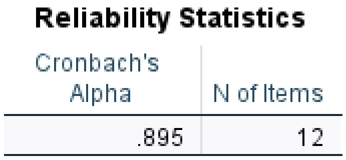
Reliability Test of CSE



Case Processing Summary

		N	%
Cases	Valid	574	98.6
	Excluded[a]	8	1.4
	Total	582	100.0

a. Listwise deletion based on all variables in the procedure.

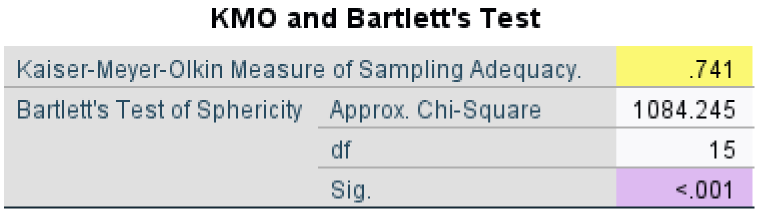


Reliability Statistics

Cronbach's Alpha	N of Items
.895	12

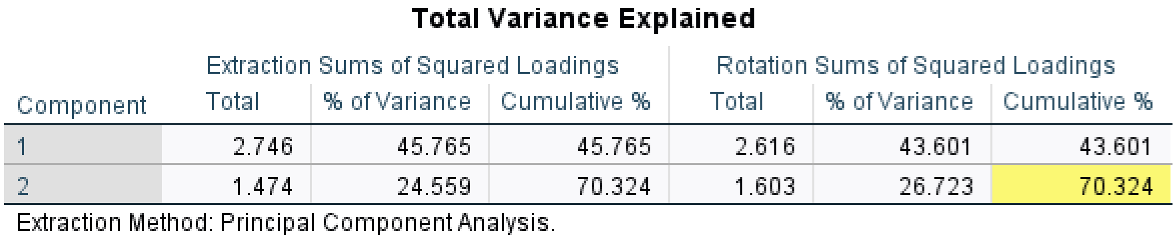
Table B12

Factor Analysis–KMO for ITU



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.741
Bartlett's Test of Sphericity	Approx. Chi-Square	1084.245
	df	15
	Sig.	<.001



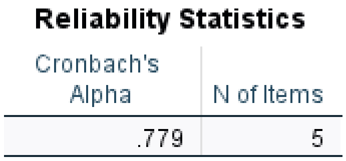
Total Variance Explained

	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.746	45.765	45.765	2.616	43.601	43.601
2	1.474	24.559	70.324	1.603	26.723	70.324

Extraction Method: Principal Component Analysis.

Table B13

Reliability Test of ITU



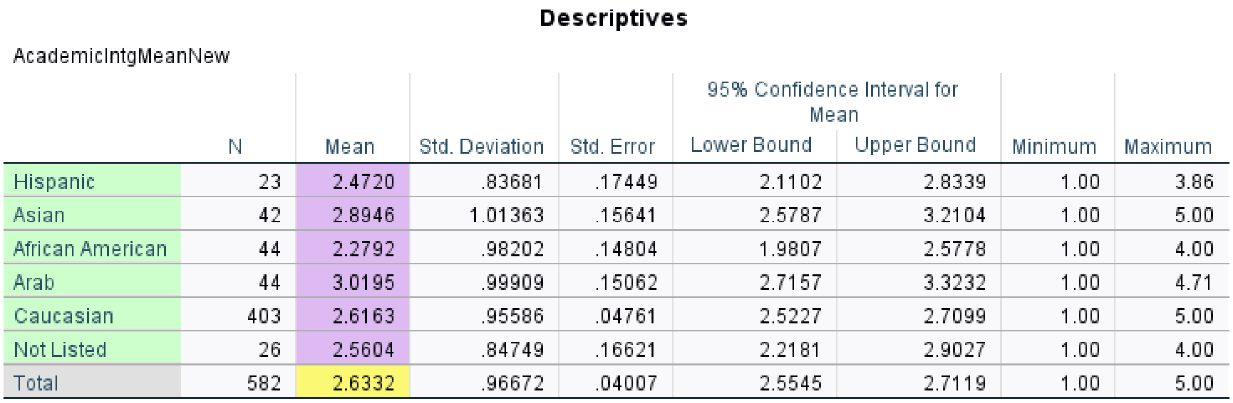
Reliability Statistics

Cronbach's Alpha	N of Items
.779	5

Appendix C: Part Two of Analysis

Table C1

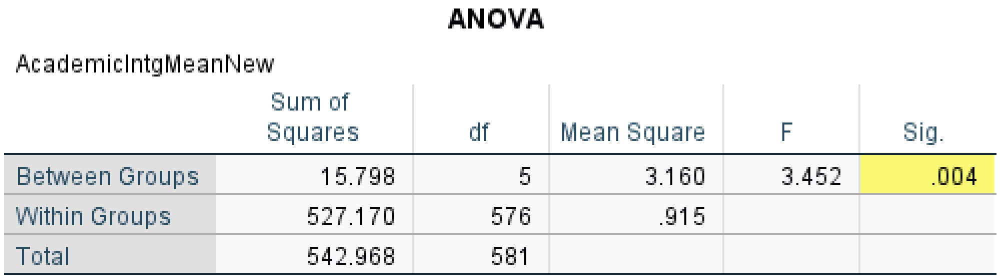
One-Way ANOVA-AI Concerns



Descriptives

AcademicIntgMeanNew

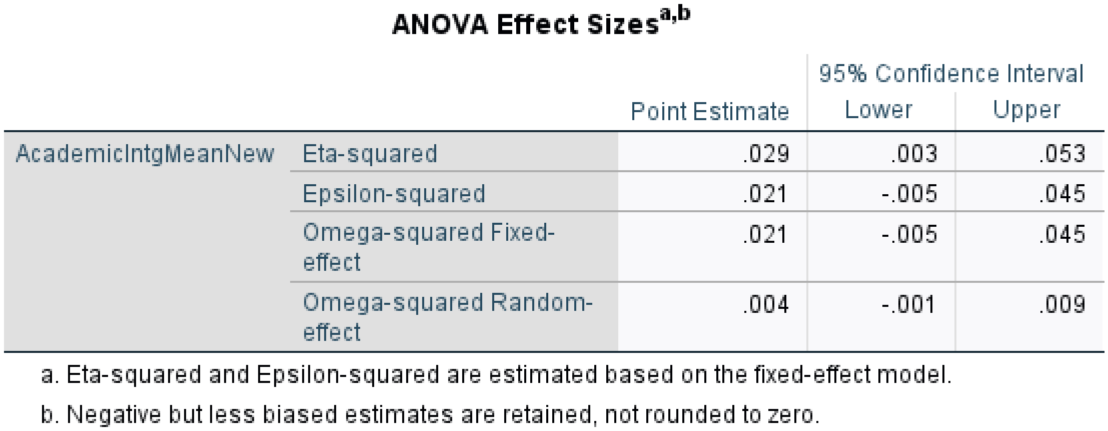
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Hispanic	23	2.4720	.83681	.17449	2.1102	2.8339	1.00	3.86
Asian	42	2.8946	1.01363	.15641	2.5787	3.2104	1.00	5.00
African American	44	2.2792	.98202	.14804	1.9807	2.5778	1.00	4.00
Arab	44	3.0195	.99909	.15062	2.7157	3.3232	1.00	4.71
Caucasian	403	2.6163	.95586	.04761	2.5227	2.7099	1.00	5.00
Not Listed	26	2.5604	.84749	.16621	2.2181	2.9027	1.00	4.00
Total	582	2.6332	.96672	.04007	2.5545	2.7119	1.00	5.00



ANOVA

AcademicIntgMeanNew

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	15.798	5	3.160	3.452	.004
Within Groups	527.170	576	.915		
Total	542.968	581			



ANOVA Effect Sizes[a,b]

		Point Estimate	95% Confidence Interval	
			Lower	Upper
AcademicIntgMeanNew	Eta-squared	.029	.003	.053
	Epsilon-squared	.021	-.005	.045
	Omega-squared Fixed-effect	.021	-.005	.045
	Omega-squared Random-effect	.004	-.001	.009

a. Eta-squared and Epsilon-squared are estimated based on the fixed-effect model.

b. Negative but less biased estimates are retained, not rounded to zero.

Table C2

Multiple Comparisons–AI Concerns by Ethnicity

Multiple Comparisons

Dependent Variable: AcademicIntgMeanNew

	(I) Ethnicity	(J) Ethnicity	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Tukey HSD	0	1	-.42251	.24816	.531	-1.1321	.2871
		2	.19283	.24616	.970	-.5110	.8967
		3	-.54743	.24616	.228	-1.2513	.1564
		4	-.14424	.20509	.982	-.7307	.4422
		5	-.08839	.27385	1.000	-.8714	.6946
	1	0	.42251	.24816	.531	-.2871	1.1321
		2	.61534*	.20638	.035	.0252	1.2054
		3	-.12492	.206	.991	-.7150	.4652
		4	.27826	.15512	.471	-.1653	.7218
		5	.33412	.23873	.727	-.3485	1.0167
	2	0	-.19283	.24616	.970	-.8967	.5110
		1	-.61534*	.20638	.035	-1.2054	-.0252
		3	-.74026*	.20396	.004	-1.3235	-.1571
		4	-.33707	.15189	.230	-.7714	.0972
		5	-.28122	.23665	.842	-.9579	.3954
	3	0	.54743	.24616	.228	-.1564	1.2513
		1	.12492	.20638	.991	-.4652	.7150
		2	.74026*	.20396	.004	.1571	1.3235
		4	.40319	.15189	.086	-.0311	.8375
		5	.45904	.23665	.379	-.2176	1.1357
	4	0	.14424	.20509	.982	-.4422	.7307
		1	-.27826	.15512	.471	-.7218	.1653
		2	.33707	.15189	.230	-.0972	.7714
		3	-.40319	.15189	.086	-.8375	.0311
		5	.05585	.19358	1.000	-.4976	.6094
	5	0	.08839	.27385	1.000	-.6946	.8714

	1	-.33412	.23873	.727	-1.0167	.3485
	2	.28122	.23665	.842	-.3954	.9579
	3	-.45904	.23665	.379	-1.1357	.2176
	4	-.05585	.19358	1.000	-.6094	.4976