Journal of Pedagogical Sociology and Psychology
Volume 6, Issue 1, 2024
https://doi.org/10.33902/jpsp.202424403

Research Article

Awareness of cyber security aspects in distance education

Hassan Hadi Al-Fatlawi

Ministry of Oil, Petroleum Research and Development Center, Baghdad, Iraq

Correspondence should be addressed to Hassan Hadi Al-Fatlawi hassan_hadima@yahoo.com

Received 23 October 2023; Revised 2 February 2024; Accepted 20 February 2024

In the ever-evolving landscape of information technology, its remarkable advancements are accompanied by a dark underbelly - the surge of digital crime. This necessitates the establishment of robust security measures within the digital realm. Cybersecurity is a pivotal technological development on the global stage, safeguarding data, networks, and electronic systems from debilitating attacks that jeopardize their integrity and wield significant influence in international relations. This study delves into assessing cyber security awareness in distance education, encompassing participants ranging from employees and university students to researchers and academics. The primary objective of this research is to underscore the pivotal role of cybersecurity education and the importance of cultivating an awareness of security threats in the education reform process. Furthermore, this paper posits the potential evolution of instructional techniques for cybersecurity through implementing machine learning and security analytics models. It provides a comprehensive overview of the contemporary cybersecurity landscape and technological advancements. Employing a quantitative descriptive analytical approach, the study reveals that participants exhibit moderate awareness regarding cyber security concepts, risks, and violations. Notably, there are no statistically significant differences at the .05 level. To enhance public awareness and facilitate active engagement in disseminating cyber security awareness, the study recommends the development of tailored distance learning curricula and the creation of sophisticated virtual learning environments. These measures are pivotal in fortifying our digital defenses and ensuring a safer digital future.

Keywords: Cybersecurity, distance education, security guarantees, cybersecurity awareness, machine learning

1. Introduction

In the last decade, the concept of cybersecurity has gained prominence as our society becomes increasingly interconnected, propelled by rapid technological advancements. While these innovations bring convenience to our daily lives, they also introduce heightened threats to the security of personal information (Dai, 2018). Cybersecurity, encompassing the protection of electronic systems from malicious attacks, has become a critical practice, covering computers, networks, servers, mobile devices, and data recovery post-assault (Poepjes & Lane, 2012). The significance of cybersecurity is underscored by its role in safeguarding personal information, maintaining employee productivity, and instilling customer trust in businesses. The roots of cybersecurity trace back to the 1970s with the inception of ARPANET, pre-dating the Internet (Simonet & Teufel, 2019). It has since evolved to address different threats, categorized into Application security, Network security, Cloud security, and Internet of Things [IoT] security. Cybersecurity is essential not only for securing data but also for protecting against theft and erasure of various data types, including sensitive information, personally identifiable information [PII], protected health information [PHI], personal data, and intellectual property assaults (Skripak et al., 2020). Moreover, it extends beyond information security to encompass the safeguarding of physical information (Villanueva et al., 2020) .The primary objectives of cybersecurity revolve around enhancing the security of operational technological systems, addressing information security threats, creating a trustworthy environment for business interactions, ensuring infrastructure resilience against electronic assaults, reducing cybercrimes, eliminating flaws in electronic systems, repairing information security system flaws, and educating individuals about new cyber-attack techniques and methods (Hadlington & Parsons, 2017; Pawlowski & Jung, 2015) . Effective cybersecurity relies on a combination of essential elements. Technology plays a crucial role in providing superior protection against cyber-attacks, utilizing various forms such as smart computers, networks with firewalls, malware protection, and antivirus measures. People also play a vital role in adhering to key data protection principles, using strong passwords, and avoiding potential risks. Processes involving operations and activities managed by both people and technologies contribute to implementing cybersecurity fundamentals (Poepjes & Lane, 2012).

There are different cybersecurity patterns focus on distinct aspects: 1) Network security (protecting computer networks against invasive and opportunistic components), 2) Application security (Ensuring the security of devices and programs to prevent unauthorized acces), and 3) Information security (Safeguarding the integrity and privacy of data at storage stages) (Skripak et al., 2020).

2. Literature Review

To maintain a high level of cybersecurity, several mechanisms and requirements are recommended, including regular backup copies of information files, the use of trusted websites for personal information, avoiding email attachments or links from unknown sources, keeping hardware up-to-date with security patches, and promoting a culture of safe internet use (Poepjes & Lane, 2012; Shaw, 2009; Yeo, 2007) .Cybersecurity awareness involves training staff members to understand the importance of protecting customer data privacy, people's identities, and other assets vulnerable to cybercriminals. It addresses risks associated with internet usage, email communication, and online interactions. Awareness training is crucial in preventing user-related security breaches, fostering a cybersecurity culture, and preparing for potential cyber-attacks (Pawlowski & Jung, 2015). Cybersecurity education is essential for investigators to quickly identify and respond to data breaches (Eminağaoğlu et al., 2009). It helps in averting the loss of personally identifiable information [PII], intellectual property, money, or brand reputation. Security awareness training is a formal process that teaches employees and stakeholders how to protect an organization's computer systems, data, customers, and other assets from online threats and criminal activity (Poepjes & Lane, 2012) .

The goals of security education include improving the response to cybersecurity incidents, reducing breaches, enhancing the effectiveness of security tools, improving employees' expertise, and understanding emerging cyber threats (Cain et al., 2018; Rezgui & Marks, 2008) .The initial stage of security awareness involves measuring the baseline level of awareness within a company before implementing security awareness training. This assessment helps tailor the training program to address specific areas of vulnerability and reinforce security measures. Implementing security awareness involves creating a behavioral reference point, activating security measures, and securing conduct from the outset (Abawajy & Kim, 2010; Al-Janabi & Al-Shourbaji, 2016; Shaw et al., 2009) .The advantages of cybersecurity awareness training include reducing the overall security risk, minimizing financial losses due to cybercrime, preventing security gaps when employees leave the organization, and maintaining a positive reputation with customers (Garba et al., 2020).

Cybercrime encompasses any illegal activity that employs a computer as its primary tool for theft and commission. Hackers, seeking access to computer networks, were among the earliest forms of cybercrime. Noteworthy cybercrimes include Ponzi Schemes, Spoofing a website, Ransomware, Malware, and IoT espionage. The cost of cybercrime has been on the rise, making cybersecurity awareness and preventive measures increasingly crucial (Amao, 2015). There are four main types of cybersecurity threats: Malware, Emoted, Phishing, SQL Injection, and Password Attacks (Nayak & Yasser, 2012). Protecting shared information from these threats requires implementing cybersecurity measures in line with Information Security Management guidelines. (Furnell & Vasileiou, 2022). Distance education, initiated in the 1970s, has witnessed significant growth with the advent of the Internet. Online courses have become increasingly popular, with millions of students opting for remote education. While there are advantages such as a variety of courses and cost-effectiveness, there are challenges, including the absence of an interactive environment and increased vulnerabilities (McDaniel, 2013; Oncu & Cakir, 2011; UAE Today, 2010). Cybersecurity has evolved into a fundamental practice in our interconnected society. Its importance is underscored by the increasing threats to personal information and its critical role in protecting data, networks, and individuals. With the growth of distance education and the rising reliance on online platforms, cybersecurity awareness becomes even more vital to mitigate risks and ensure the security of digital environments. As online education continues to evolve, the study anticipates future challenges and proposes solutions. It calls for collaborative efforts to address the shortage of cybersecurity experts, especially those skilled in artificial intelligence and distance learning. The development of a skilled workforce is crucial for maintaining network security and adapting to the dynamic cyber landscape.

The research contributes valuable insights into the current state of cyber security awareness in distance education and provides a roadmap for enhancing education, training, and awareness programs. By prioritizing cyber security in educational initiatives, we can build a safer digital future, protect sensitive information, and mitigate the risks associated with cyber threats in the evolving landscape of online education.

3. Materials and methods

In this study, which was conducted to determine the trends and levels of awareness of cyber security in distance education, the target group included employees, university students, researchers, and academics.

3.1. Data Collection & Data Analysis

The bedrock of robust cybersecurity lies in the meticulous collection and analysis of data using specialized instruments. By capturing the vast, dynamic flow of information within your systems through tools like Security Information and Event Management [SIEM] systems, intrusion detection/prevention systems (IDS/IPS], and threat intelligence feeds, you gain the critical ability to proactively detect and neutralize security threats before they inflict damage. This data empowers you on multiple fronts: identifying the ever-shifting terrain of cybercrime by analyzing network traffic, user activity, and system logs, fortifying your defenses by continuously upgrading and maintaining security infrastructure based on data-driven insights, and responding to incidents with swift precision through techniques like user behavior analytics and attack timeline reconstruction. Gathering this essential information can involve a spectrum of techniques, from structured surveys and in-depth interviews to vigilant observation of user behavior and meticulous analysis of existing data repositories. Regardless of the method, the ultimate goal remains constant: to fuel proactive cybersecurity strategies that anticipate, identify, and neutralize even the most sophisticated cyberattacks, ultimately safeguarding your organization and its valuable assets.

3.2. Statistical Analysis

A total of 300 individuals participated in the study. Of these, 169 (56.3%) were men and 131 (43.7%) were women. The participants' demographic profile is summarized in Table 1. The selection of these person groups, who use information systems as part of their daily job requirements, was predicated on the assumption that they were more concerned with their private information in the academic sectors, such as students' grades, tests, research records, etc. The convenience sampling approach, which falls under the non-probability sampling category, was used for the current investigation. The advantage of this sampling strategy is that it is quick and convenient. The term "convenience sampling technique" refers to sampling strategies where a sample of the population who are easily accessible to reply is used (Hair et al., 2018).

Table 1
Demographic profiles of the participants

Characteristic	*Frequency*	*Percentage*
Gender		
Male	169	56.3
Female	131	43.7
Age		
18-29 years old	118	39.3
30-39 years old	96	32.0
40-49 years old	63	21.0
Above 50 years old	23	7.7

In this study, it was used two statistical packages for analyzing the data.

(1) For the descriptive analysis, it was done using the SPSS (Statistical Package for the Social Sciences) application.

(2) With the aid of the Study Moment of Structures [AMOS] program, structural equation modeling [SEM] analysis was carried out. Structural equation modeling is the most effective multivariate technique for analyzing both the construct validity and theoretical connections (SEM). SEM is a more persuasive method than other types of analysis of covariance. It went on to say that since SEM takes measurement errors into account, the strength of connections between constructs might be determined with more accuracy (Kruger et al., 2010). However, several formal procedures must be followed in SEM. SEM offers a theoretically compelling method for carefully testing a theory about the connections between variables and latent components. Information Security Awareness Capability Model [ISACM] and Situation Awareness-Oriented Cyber security Education are two popular models that we used in this work Awareness-Oriented Cyber security Education [SAOCE]. SEM may demonstrate how well the theory matches the facts when it is presented. Additionally, SEM generates reliable data free of measurement mistakes (Zainudin, 2015).

SEM programs provide estimates and tests of the free coefficients, while the fixed coefficients contribute importantly to testing the overall model structure. Various kinds of constraints between coefficients can also be used .

When conducting a structural equation model or confirmatory factor analysis [CFA], it is often recommended to test for multivariate normality. Some popular SEM software packages (such as AMOS) assume your variables are continuous and produce the best results when data are normally distributed .

The major assumptions associated with structural equation modeling include: multivariate normality, no systematic missing data, sufficiently large sample size, and correct model specification. Nearly all of the inferential statistics (e.g., t-tests, ANOVA, simple regression, and MRC) rely upon something that is called the “Assumption of Normality'.

4. Results

The survey participants agree that investing in cyber training exposes them to cyber threats, even though acquiring cyber awareness demands both financial resources and effort. In theory, individuals tend to be more cautious and adept at preventing cyber-attacks when the available cyber tools are user-friendly and familiar, as suggested by previous researchers. However, challenges arise when using cyber tools requiring sophisticated or specialized expertise. Earlier studies indicate that individuals, particularly students, are more vulnerable to cybercrime when lacking awareness. Due to the global pandemic, all necessary teaching and learning activities had to transition online. The effectiveness of Open and Distance Learning [ODL] implementation hinges on sufficient security awareness. The measurement model follows the Confirmatory Factor Analysis. Next, we will assess the structural model to validate our hypothesis (Zainudin, 2015). Finally, we conducted procedures to address common method variance [CMV] using Harman's

One Factor Solution analysis. Table 2 displays a summary of the model fit for the measurement model.

Table 2
Result of Measurement Model

	AFI		*IFI*		*PFI*
Fit Indices	Relative Chi Square [<5]	RMSEA [<=0.080]	CFI [>=0.900]	TLI [>=0.900]	PGFI [>=0.500]
Measurement Model	2.495	0.060	0.954	0.946	0.703

Note. AFI stands for absolute fit index, IFI for incremental fit index, and PFI for sparse fit index. Root mean square error of approximation [RMSEA], comparative fit index [CFI], Tucker-Lewis index [TLI], and parsimonious goodness of fit index [PGFI] are acronyms.

The descriptive approach was applied by the researcher in this investigation. We also evaluated the measurement model's construct reliability, discriminant validity, and convergent validity. A group of variables or items that are thought to assess a construct and have a significant amount of shared variation are said to have convergent validity.

Five dimensions were identified to study the factors affecting the achievement of cyber security among students and educators, namely PV, PS, PSE, PRE, and PC of cyber security awareness, which theoretically supported the association with cyber behavior. Our findings show that the PV and PSE of responders have a significant correlation with cyber security behavior; it was found there is no connection between PS and PRE on cyber security behavior according to (Patel et al., 2015; Pawlowski Jung, 2015). In the measurement model, the researcher relied on convergent and composite reliability, and its results are evident in Tables 3 and 4.

Table 3
Convergent Validity and Composite Reliability [CR] Results

Constructs	*Items*	*Factor loadings (>0.500)*	*AVE (>0.500)*	*CR*
Perceived Vulnerability [PV]	PV1	0.844	0.642	0.843
	PV2	0.831		
	PV3	0.723		
Perceived Severity [PS]	PS1	0.718	0.600	0.818
	PS2	0.818		
	PS3	0.784		
Perceived Self-Efficacy [PSE]	PSE1	0.932	0.794	0.939
	PSE2	0.928		
	PSE3	0.846		
	PSE4	0.855		
Perceived Response Efficacy [PRE]	PRE1	0.798	0.696	0.902
	PRE2	0.821		
	PRE3	0.882		
	PRE4	0.835		
Perceived Costs [PC]	PC1	0.854	0.663	0.887
	PC2	0.798		
	PC3	0.822		
	PC4	0.781		
Cyber security Behavior [CB]	CB1	0.877	0.746	0.936
	CB2	0.888		
	CB3	0.848		
	CB4	0.890		
	CB5	0.814		

In the second phase of SEM, the structural model is tested by looking at the predicted associations between latent variables. One endogenous relationship connecting the variables of the hypothesized model is indicated by the structural model. Table 4 of the results shows a range of outcomes. The purpose of the constructs' discriminant validity is to reveal if the items are redundant. Additionally, results revealed that the r2 values of all variables are lower than AVEs, as shown in Table 4 when comparing the r2 values with the AVE value, these results were in agreement with those reported by (Skripak, 2020; Villanueva et al., 2020).

Table 4

Convergent Validity and Composite Reliability Result

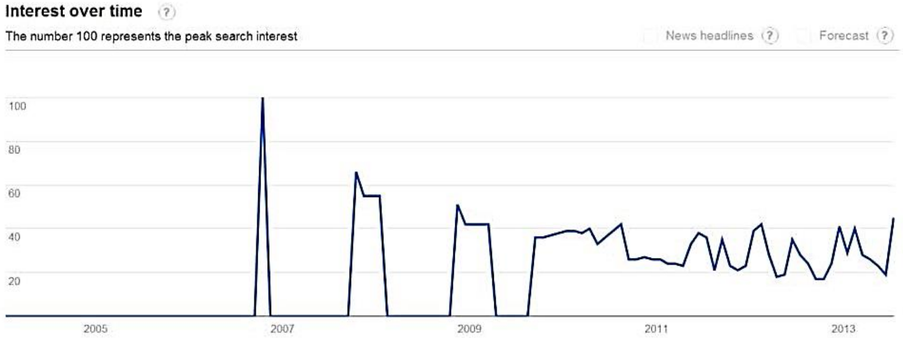
Tested path		*AVE1*	*AVE2*	*Result*
PV	PS	0.642	0.600	Valid
PV	PSE	0.642	0.794	Valid
PV	PRE	0.642	0.696	Valid
PV	PC	0.642	0.663	Valid
PS	PSE	0.600	0.794	Valid
PS	PRE	0.600	0.696	Valid
PS	PC	0.600	0.663	Valid
PS	CB	0.600	0.746	Valid
PSE	PRE	0.794	0.696	Valid
PSE	PC	0.794	0.663	Valid
PSE	CB	0.794	0.746	Valid
PRE	PC	0.696	0.663	Valid
PRE	CB	0.696	0.746	Valid
PC	CB	0.663	0.746	Valid
PV	CB	0.642	0.746	Valid

Note. Perceived vulnerability [PV], perceived severity [PS], perceived self-efficacy [PSE], perceived response effectiveness [PRE], perceived cost [PC], perceived behavior [CB], and average variance extracted [AVE] are all included.

To track Internet users' search interests regarding "online learning security" in recent years, we applied Google Trends, a web-based search tool that provides the frequency of some specific search terms or keywords queried over a specific period. The result generated by Google Trends (see Figure 1) indicated that although the search frequency of online learning security has fluctuated in a narrow range since 2010, the overall attention paid to it has not changed much. This was consistent with the result we got via a Google Blog search.

Figure 1

Frequency of searches for "online learning security (Chen & He, 2013, p.113)



A thorough literature search using academic databases and Google Scholar revealed that there are several security hazards associated with online learning (Table 5), the majority of which are caused by outside attackers.

Table 5

Security Risks and Protection Measures in Distance Education

Security risks	*Protection measures*
MITM attack and poisoning of the ARP cache Use of force offensive Cross-Site Request Forgery [CSRF] Cross-Site Scripting [XSS] Denial of Service [Dos] IP spoofing Masquerade Rootkits Query Injection Hijacking of a session Session Prognosis	Equipping computers with antivirus and firewall software (Weippl & Ebner, 2008) Putting Security Management [ISM] into Practice (Adams & Blandford, 2003; Alwi & Fan, 2010) Enhancing secrecy, accountability, authorization, and authenticity (Agulla et al., 2008) Making use of digital rights management and cryptography (Barik & Karforma, 2012) Professional security training (Srivastava & Sinha, 2013) Attacks that stack-smash (Barik & Karforma, 2012; Costinela-Luminita & Nicoleta-Magdalena, 2012; Srivastava & Sinha, 2013)

5. Discussion

The researcher believes that increasing the level of awareness of cyber security at the lower age group who are in the education stage and have not joined the labor market can be a basis for building awareness of the importance and danger of cyber security in society. There is no doubt that when they join the work, this awareness will crystallize in them effectively. Better results can be obtained when the teaching of cyber security is in the pre-university stages of study. The researcher asserts that the lack of sufficient awareness of the importance of cyber security applications among the participants in the study may be due to the fact that the warnings of threats facing information security in general focus on banking sectors and large entities in society without highlighting the personal importance of cyber security at the individual level. This is a big mistake as personal awareness of this problem is part of public awareness. The researcher also directs the great role of educational policies in developing societal awareness of cyber security through qualifying courses for teachers to pass them on to students. In the absence of an interactive climate in distance education, by creating intellectual interaction between teachers and students is a better advantage than in-person interaction.

The problem that hinders the development of awareness of the importance of cyber security and the potential threats to information security involves the disparity between individuals in the importance of cyber security in society and the requirements of daily life, as the motives that exist among bank and corporate employees are different from those of students or security institutions, for example. Accordingly, each of these categories must be dealt with in terms of the direct impact of cyber security on their work, and the case of students in particular, teachers should pay attention to developing students' creativity in terms of their perceptions to deal with risks that threaten their personal information and develop skills to address them, and from On the other hand, their awareness of the advantages of the digital environment in educational programs, the need to preserve them, and the danger of penetration by hackers.

There is an urgent need for more cybersecurity experts in the field of artificial intelligence and distance learning who are able to work with programming at this scale. The staff that can keep the distance learning network up to date and make necessary modifications will be very helpful to its security. Although there is a significant global need for people who can deliver these solutions, the pool of competent and trained people that is accessible is fewer than this (McDaniel, 2013; Yeo et al., 2007).

We used Google Trends, a web-based search engine that displays the frequency of certain specific search phrases or keywords questioned over a specific period, to monitor Internet users' search interests about "online learning security" in recent years. The outcome produced by Google Trends showed that although the general level of interest in online learning security has not changed considerably since 2010, it has varied in a limited range in terms of search frequency. This was in line with the outcome of a Google Blog search (Chen & He, 2020).

The study results indicate that there is a correlation between the age of the participants in the study and the level of cyber security awareness, with significant differences between the different age groups, where the level of awareness was high in the group (18 - 29) years old, while it was low in the group (40 - 49) years old and low by a degree large for the 50-year-olds group. The obtained results were similar to those reported by (McDaniel, 2013; Yeo et al., 2007).

The awareness of cyber security aspects in distance education is a critical dimension that warrants further discussion, considering the evolving landscape of technology and online learning environments. As the reliance on digital platforms for education continues to grow, understanding and addressing cybersecurity concerns become paramount. One key aspect that emerges from the study is the significant correlation between age groups and cyber security awareness. The finding that younger individuals, particularly those in the 18 to 29 age brackets, exhibit higher levels of awareness implies that efforts to integrate cybersecurity education should be targeted at specific demographics. Tailoring awareness campaigns to the needs and characteristics of different age groups can contribute to more effective education and prevention strategies. Moreover, the study sheds light on the pivotal role of education policies in shaping societal awareness of cyber security. Implementing qualification courses for teachers not only equips them with the necessary knowledge but also positions them as key influencers in disseminating cybersecurity concepts to students. The emphasis on intellectual interaction in distance education underscores the importance of creating an engaging online learning environment that not only imparts knowledge but also fosters a culture of cyber security consciousness (Al-Janabi, & Al-Shourbaji, 2016). The disparity in motivations among individuals, highlighted in the study, underscores the need for a nuanced approach to cyber security awareness. Recognizing that different groups, such as bank employees, corporate professionals, students, and security institutions, may have varied motivations and concerns is crucial. Customizing awareness programs to address the specific impact of cyber security on each group is essential for fostering a comprehensive understanding of the risks and preventive measures. The shortage of cyber security experts, particularly in areas like artificial intelligence and distance learning, is a pressing concern that emerges from the study. As educational institutions increasingly adopt online learning platforms and integrate technologies like AI, the demand for experts who can navigate the intricate cybersecurity landscape becomes imperative. Efforts should be directed towards bridging this gap by offering specialized training programs and encouraging more individuals to pursue careers in cyber security. The use of Google Trends to analyze search interests related to "online learning security" provides insights into the broader societal interest in this domain. While the overall interest has remained stable, the variation in search frequencies suggests fluctuations in public attention. This observation prompts further exploration into the factors influencing public interest and the potential correlation between external events and spikes in interest (Varakuti, & Shwethashri, 2023).

In conclusion, the discussion surrounding awareness of cyber security aspects in distance education extends beyond the immediate findings of the study. It delves into the need for targeted education strategies, the role of educators in shaping awareness, the importance of nuanced approaches for different groups, the urgency in addressing the shortage of cybersecurity experts, and the dynamic nature of public interest in online learning security. As the digital landscape evolves, continually refining and advancing cyber security awareness in distance education remains a critical endeavor.

6. Conclusion

Online education has developed significantly during the last ten years. Perhaps the growth was too rapid, and the security of the organization received little attention. Thanks to new technology, online education will become more user-centered and safe.

In this study, 5 dimensions of cyber security awareness that affect cyber security behavior in distance education policy are explored. Unfortunately, there were few theoretical and empirical investigations on the association between situations that encourage cyber activity found in the literature for these variables. There was little empirical data on cybersecurity behavior.

The results should be interpreted within the parameters of the methodology used; while quantitative research methods can be used to determine the extent to which individuals engage in behaviors, they have limitations when it comes to the ability to analyze participants' thoughts and feelings as well as the interpretations they give to their experiences. To better understand cyber security behavior in the future, a mixed-method approach should be used to combine quantitative and qualitative data.

It is noted that the response to cyber security awareness among the participants in the study increases in males than in females, and gradually decreases with increasing age.

Information security in the online education sector lags well behind other industries, despite technological advancements. Despite the particular difficulties that come with online education, there are luckily just a few concerns that need to be addressed in terms of information security.

The good news is that making straightforward adjustments, like including encryption in the process of developing security awareness programs for online educational institutions, will offer the much-needed support for the security awareness programs that are now ineffective. Generally, by utilizing the Information Security Awareness Capability Model and Situation Awareness-Oriented Cyber Security Education Model, we can:

(1) Create safety features for online learning.

(2) Construct a theoretical model of security behavior that is advantageous to the ODL technique.

Figure 2 illustrates the general block diagram for "Enhancing Cybersecurity Education in Distance Learning: A Machine Learning Approach", which it is contains:

1. *Input*:

- Target Audience: Employees, university students, researchers, academics
- Assessment Data: Surveys, exams, quizzes, online interactions on cybersecurity topics
- Machine Learning Models: Classification, regression, clustering algorithms

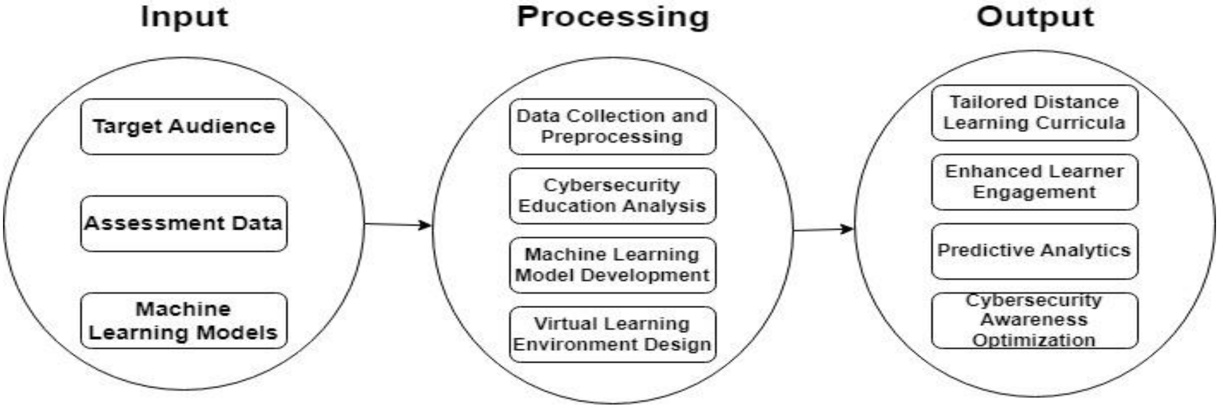
2. *Processing*:

- Data Collection and Preprocessing: Gather data from various sources, clean and format it for analysis.
- Cybersecurity Education Analysis: Evaluate current distance learning methods for cybersecurity education, and assess participants' awareness levels of cybersecurity concepts, risks, and violations.
- Machine Learning Model Development: Train models to identify patterns in learner behavior and responses, predict learning outcomes, and recommend personalized learning paths.
- Virtual Learning Environment Design: Develop interactive and engaging virtual learning environments for cybersecurity education, utilizing gamification, simulations, and personalized feedback mechanisms.

3. *Output*:

- Tailored Distance Learning Curricula: Personalized learning modules and pathways based on individual needs and learning styles.
- Enhanced Learner Engagement: Improved motivation and participation in cybersecurity education through interactive virtual environments.
- Predictive Analytics: Identifying potential gaps in awareness and risks of individual learners and groups.
- Cybersecurity Awareness Optimization: Continuous improvement of distance learning methods and virtual environments based on data insights and machine learning predictions.

Figure 2
General overview of the framework


Input
Processing
Output
Target Audience
Assessment Data
Machine Learning Models
Data Collection and Preprocessing
Cybersecurity Education Analysis
Machine Learning Model Development
Virtual Learning Environment Design
Tailored Distance Learning Curricula
Enhanced Learner Engagement
Predictive Analytics
Cybersecurity Awareness Optimization

7. Recommendations

The importance of cyber security in distance education has been clearly demonstrated during the coronavirus pandemic that recently swept the world, and it has added more importance to awareness of it than it was previously limited to securing information in banks, companies, and institutions concerned with information in society, and some suggestions can be made that help to having a good awareness and knowledge of the basics of cyber security:

1 - Outlining and developing a new curriculum for education that is appropriate for distance learning, developing a cutting-edge virtual learning environment, and rethinking the student in general, including the experience of extracurricular activities.

2 - Avoid opening anonymous links, and use the encryption system to open some suspicious sites to encrypt their communications.

3 - Benefit from the experiences of the leading countries in the field of distance education in a way that helps to overcome the weaknesses that allow hackers to penetrate the information infrastructure, and since cyber-attacks are constantly evolving and the losses resulting from these attacks outweigh the potential material losses, so the existing programs must be developed in return. The educational institutions are constantly.

Declaration of interest: No conflict of interest is declared by the author.

Funding: No funding was received for undertaking this study.

References

Abawajy, J., & Kim, T. H. (2010). Performance analysis of cyber security awareness delivery methods. In T. Kim, W. Fang, M. K. Khan, K. P. Arnett, H. Kang, & D. Slezak (Eds.), *Security technology, disaster recovery, and business continuity* (pp. 142-148). Springer. https://doi.org/10.1007/978-3-642-17610-4_16

Adams, A. and Blandford, A. (2003). Security and online learning: to protect or prohibit. In C. Ghaoui (Ed.), *Usability evaluation of online learning programs* (pp. 331–359). IDEA Publishing. https://doi.org/10.4018/978-1-59140-105-6.ch018

Agulla, E. G., Rifón, L. A., Castro, J. L. A., & Mateo, C. G. (2008). Is my student at the other side? Applying biometric web authentication to e-learning environments. In Commission (Ed.), *2008 Eighth IEEE international conference on advanced learning technologies* (pp. 551-553). IEEE. https://doi.org/10.1109/ICALT.2008.184

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information & Knowledge Management, 15(01),* 1650007. https://doi.org/10.1142/S0219649216500076

Alwi, N.H., Fan, I. S. (2010). Information security threats analysis for e-learning. In M. D. Lytras

(Ed.), *Technology enhanced learning. quality of teaching and educational reform. TECH-EDUCATION 2010*: *Communications in computer and information science*. Springer. https://doi.org/10.1007/978-3-642-13166-0_41

Amao, S. (2015). *Active cyber defense to fight cybercrime* (Publication No. 1606336) [Master's thesis, Utica College]. ProQuest Dissertations and Theses Global.

Barik, N., & Karforma, S. (2012). Risks and remedies in e-learning system. *International Journal of Network Security & Its Applications*, *4*(1), 51-59. https://doi.org/10.5121/ijnsa.2012.4105

Cain, A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security Applications, 42,* 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

Chen, Y. & He, W. (2013). Security Risks and Protection in Online Learning: A Survey. *The International Review of Research in Open and Distance Learning, 14*(5), 109-127. https://doi.org/10.19173/irrodl.v14i5.1632

Costinela-Luminița, C. D., & Nicoleta-Magdalena, C. I. (2012). E-learning security vulnerabilities. *Procedia-Social and Behavioral Sciences, 46,* 2297-2301. https://doi.org/10.1016/j.sbspro.2012.05.474

Dai, J. (2018). Situation awareness-oriented cyber security education. *IEEE Frontiers in Education Conference, 2018,* 1-8. https://doi.org/10.1109/FIE.2018.8658929

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – a case study. *Information Security Technical Report, 14,* 223-229. https://doi.org/10.1016/j.istr.2010.05.002

Furnell, S. M., & Vasileiou, I. (2022). A holistic view of cyber security education requirements. In M. Khosrow-Pour (Eds.), *Research anthology on advancements in cybersecurity education* (pp. 289–307). IGI Global. https://doi.org/10.4018/978-1-6684-3554-0.ch013

Garba, A., Maheyzah, B., Siti, H., & Dauda, I. (2020). Cyber security awareness among university students: a case study. *Journal of Science Proceedings Series, 2*(1), 82-86. https://doi.org/10.31580/sps.v2i1.1320

Hadlington, L. & Parsons, K. (2017). Can cyberloafing and internet addiction affect organizational information security? *Cyberpsychology, Behavior, and Social Networking, 20*(9), 567-571. https://doi.org/10.1089/cyber.2017.0239

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2018). *Multivariate data analysis.* Cengage Learning, EMEA.

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*(5), 316–327. https://doi.org/10.1108/09685221011095236

McDaniel, E. A. (2013). Securing the information and communications technology global supply chain from exploitation: Developing a strategy for education, training, and awareness. *Issues in Informing Science and Information Technology, 10,* 313–324. https://doi.org/10.28945/1813

Nayak, M., & Yasser, L. (2012). Cybercrime: A threat to network security. *Internal Security Journal, 12*(2), 84-88. https://doi.org/10.1016/S1353-4858(12)70020-X

Oncu, S., & Cakir, H. (2011). Research in online learning environments: Priorities and methodologies. *Computers & Education, 57*(1), 1098-1108. https://doi.org/10.1016/j.compedu.2010.12.009

Patel, A., Al-Janabi, S., AlShourbaji, I., & Pedersen, J. (2015). A novel methodology towards a trusted environment in mashup web applications. *Computers & Security, 49,* 107–122. https://doi.org/10.1016/j.cose.2014.10.009

Pawlowski, S.D. & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education, 26,* 281-294.

Poepjes, R., & Lane, M. (2012). *An information security awareness capability model (ISACM)* [Paper presentation]. 10th Australian Information Security Management Conference, AISM 2012.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7–8), 241–253.

https://doi.org/10.1016/j.cose.2008.07.008

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computer Education, 52,* 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Simonet, J., & Teufel, S. (2019). The influence of organizational, social, and personal factors on cybersecurity awareness and behavior of home computer users. In G. Dhillon (Ed.), SEC *2019, IFIP AICT, 562,* 194–208. https://doi.org/10.1007/978-3-030-22312-0_14

Skripak, I. A., Aynazarova, S. N., Vladimirovna, E., Tkachenko, A. E., & Erina, L. S. (2020). Digital virtualization technologies in distance learning. *Advanced Trends in Computer Science and Engineering, 9*(2), 1808–1813. https://doi.org/10.30534/ijatcse/2020/138922020

Srivastava, A., & Sinha, S. (2013). Information security through e-learning using VTE. *International Journal of Electronics and Computer Science Engineering, 2*(18), 528-531.

UAE Today. (2010). *Internet virus infects Ministry of Education.* Emaratalyoum. http://www.emaratalyoum.com

Varakuti, D., & Shwethashri, K. (2023). Cybersecurity Awareness in Online Education: A Case Study Analysis. *International Research Journal of Modernization in Engineering Technology and Science, 5(7),* 1785.

Villanueva, J. A., Lacatan, L. L., Vinluan, A. A. (2020). Information technology security infrastructure malware detector system. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(2), 1583–1587. https://doi.org/10.30534/ijatcse/2020/103922020

Weippl, E. & Ebner, M. (2008). *Security & privacy challenges in e-learning 2.0* [Paper presentation]. E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, Las Vegas, Nevada.

Yeo, A. C., Rahim, M. M. & Miri, L. (2007). *Understanding factors affecting the success of information security risk assessment: The case of an Australian higher educational institution* [Paper presentation]. Pacific Asia Conference on Information Systems (PACIS), New Zealand.

Zainudin, A. (2015). *SEM made simple: a gentle approach to learning structural equation modeling*. MPWS Rich Publication.