International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

Available Online at : www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

Cyber Security Awareness in Online Education : A Case Study Analysis

[1]N Satyanandam, [2]Veldi Sriya, [3]Cheripally Shravani

[1]Associate Professor, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India

[2,3] Students, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, Telangana, India

ARTICLEINFO

Article History :

Accepted: 10 June 2023
Published: 04 July 2023

Publication Issue :
Volume 10, Issue 4
July-August-2023

Page Number :
01-08

ABSTRACT

The great technological development and digital transformations that the world is witnessing increase the rate of cyber threats and cybercrime, and due to the Covid19 pandemic, education, and commerce have relied on the Internet for the continuation of education and to maintain the economy. Threats arising from the behaviors of the individuals are among the main cyber threats, this appears from the limited awareness of individuals about cyber security and its threats. This survey paper discusses the importance of enhancing cyber security awareness among university students in Saudi Arabia to reduce cyber threats. As cyber security awareness is one of the areas of cyber security controls that aim to enhance awareness of cyber security, its threats, and risks, and build a positive cyber security culture. In addition, cyber security awareness is an important component of ensuring the protection and privacy of critical information assets. Students' awareness of cyber security, its threats, and risks enhances students' references to action when facing cybercrime to protect the information, and technology assets to reach safe cyberspace to achieve the Saudi Arabia Vision of 2030.

Keywords : Cyber Security Awareness, Cyber Threats, Enhance Cyber Security, Cyber Security, Higher Education Students.

I. INTRODUCTION

The great technological development and digital transformations that the world is witnessing increase the proportion of cyber threats and cybercrimes. Because of the Covid-19, total dependence on (distance education, e-government, e-commerce, and many others) has become on the Internet, this opens the way for a focus on enhancing cyber security awareness. Cyber security is defined as the process that includes several different processes in protecting basic software, processes, and technologies, data from damage, infection, or unauthorized access, people, and devices [1]. In addition, enhancing cyber security is one of the basic controls that have been published for cyber security controls by the National Cyber Security Authority, which consisted of several sub-controls, including (asset management, management of login

identities and powers, mobile device security, e mail protection, and others) [2]. The Saudi Minister of Trade and Investment, Dr. Majid bin Abdullah Al-Qasabi, confirmed in his speech in February 2020 that cyber threats in the region are increasing, and that the Kingdom is the most targeted, which requires double action to combat threats. However, organizations incur higher costs in handling cyber security incidents. The author in [3] said Saudi Arabia has tightened its cyber defenses, and the government has established a National Computer Emergency Response Team (CERT), which is responsible for raising public awareness of cyber security, responding to major incidents, and monitoring threats.

Tianfield [4] defined cyber security situational awareness (CSSA), awareness is an intelligence-based contextual understanding, situational awareness as the understanding of what is happening, how it has developed in recent times, and how it can go away in a short time. From a methodological point of view, the perception of the situation is achieved through the application of appropriate mechanisms of assessment, evaluation, and inference, to generate an understanding of the situation. There has been a growing focus in recent years on the role of individual behavior in minimizing cyber risks. However, the understanding of how individuals differ in their cyber security awareness, knowledge, and behavior is still very limited, when faced with diverse cyber risks [5]. The author in [6] demonstrated that awareness of data privacy is one of the main problems related to data privacy. However, most college students are not aware of data privacy issues. Since it can reveal a lot of private data due to users' data breaches, and the potential for attackers to tamper with emails and deceive users onto a fake domain site where they can monitor users' passwords and logins, it is imperative to promote data privacy awareness of its importance. Most groups that use a network are university students, so they must be the most aware of cyber security, and at an early stage, a culture of cyber security awareness must be created to form their experience before they enter the workforce [7]. Academic institutions are an important part of preparing and educating the cyber security workforce. The current research aims to enhance the awareness of University students about the correct practices in cyber security, the students were selected because they are the future employees of the organizations [8].

II. RELATED WORK

The concept of awareness first appeared in the theory of innovation diffusion [9], and awareness is defined as the extent to which the target population is aware and the formulation of a general perception of what it entails, and this means that awareness is a precedent for behavioral attitudes and intentions [10]. Situation Awareness SA, defined according to [11], is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status shortly. As explained by [12] situational awareness is on three hierarchical levels of situation assessment, each stage being a precursor to the next higher level. He mentioned [4] levels of situational awareness in (figure 1) as follows:

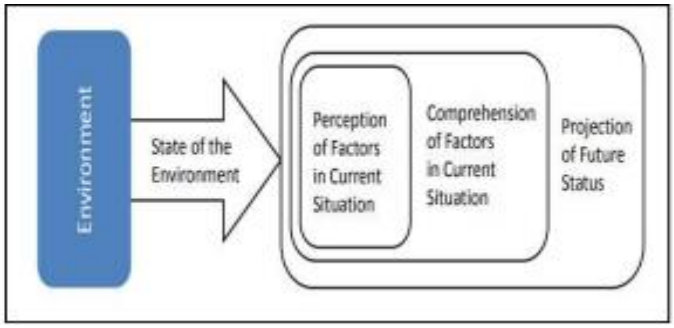

Figure 1: Layers of situational awareness.

2.1 Perception

The first layer includes perceptions of the critical factors in the environment that are important to the decision-maker. Perception involves assessing and defining the state, characteristics, and dynamics of

relevant factors in time and space based on data collected from various sources in the environment.

2.2 Comprehension

The second layer includes the factors of the first layer. It includes the integration, understanding, and association of the disjointed elements that must be understood to make a sound decision in the context of the decision maker's role.

2.3 Projection

The third layer presents understanding the situation in the future to predict the impact of those elements in the future decision context of the decision maker's vision. Both the first and second layers of management and projection involve knowledge of the state and dynamics of factors and an understanding of the elements that characterize a situation to predict what will happen in the environment over some time. [13] described it as a model that presents situational awareness as a dynamic interaction between the environment and humans. Also, the information processing approach is best represented by it, the three-level model of situational awareness was developed to understand flight tasks [14]. With technological development, it can be used to regulate human performance, and in behavior that requires cognitive tasks, to increase the capabilities of humans to act as decision-makers [12].

III. PROPOSED SYSTEM

There are many different instructional design models, such as Gagne's Nine Events of Instruction (Gagne et al., 2005), Merrill's Principles of Instruction (Mer-rill, 2002) and the ADDIE model (Campbell, 2014).

Our research objective was to analyse the current CSA level and design a culturally effective CSA course for the high-school students of Hormozgan, Iran. As an overall instructional design approach, we selected a widely known ADDIE model (Campbell, 2014), see Table 1. However, as we aimed to include cultural aspects in this research, we applied the enhanced ADDIE model with cultural embrace elements (Thomas et al., 2003), see Figure 1. This instructional model follows the principle that "the effective design of instruction would have to be grounded in a rich understanding of culture and its essential role in the socially mediated construction of reality" (Thomas et al., 2003). This covers the three I's:(1) Intention (i.e., we design in manner that is culturally sensitive and grounded in the notion of culture), (2) Interaction (i.e., more interaction with the culture we have, the more culturally appropriate and sensitive products we design) and Introspection (i.e.,we must consider our own thoughts, beliefs, attitudes, desires, and feelings toward the cultures we design for) (Thomas et al., 2003)

Stage	Description
Analyse	The process of defining what is to be learned
Design	The process of specifying how it is to be learned
Develop	The process of authoring and producing learning materials
Implement	The process of installing the instruction product in a real-world context
Evaluate	The process of determining the impact of the instruction

Table 1: ADDIE Model's Elements (Campbell, 2014)

We followed all stages of the ADDIE model, and a combination of quantitative and qualitative research methods were used in order to ensure integrity and validity of the research. As the main methods in Analyse step, a quantitative survey and interviews were con ducted. In Evaluate step pre-and post-test approach was instrumented.

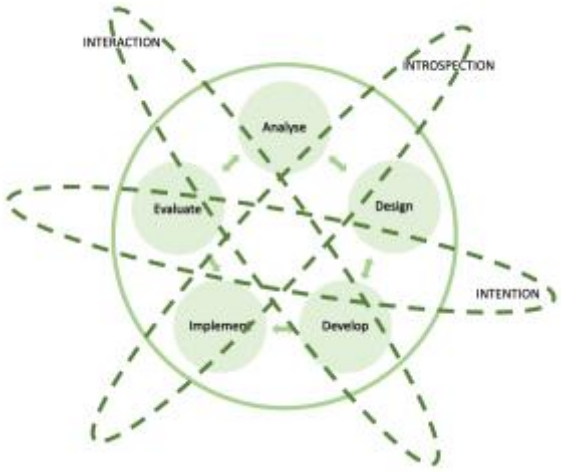

Figure 1 : ADDIE model with culture elements (Thomaset al., 2003)

IV. RESULTS AND DISCUSSION

A quantitative multiple-choice Google Forms questionnaire was developed in the Persian language and distributed via school teachers and principals to high school students. Based on 2017 data, there were a total of 49,937 students in upper secondary school (aged 16-18) and 74,237 students in lower secondary school (aged 13-15) in Hormozgan7, with the total population approx.124,000 students. A total of 616 responses were collected from students aged 13-18. In accordance to the sample sizes guidance in Internet surveys, the 616 answers collected from the questionnaire were sufficient to demonstrate statistical significance (Hill, 1998). In addition an interview with one of the high-school principals was organized to validate the data collected with the expert views and to acquire supplementary information. However, no details or personalised data from the course was shared with the principal to en sure impartiality and validity of research.

The questionnaire captures the students' existing knowledge on the CSA topics following the main cyber security threats in Iran (Shoja Heydari, 2015), including clicking unknown links, backups, VPN security, password security, abuse of the unattended de vice, phone anti-viruses, software updates, phishing attacks, being hacked and cyber bullying.

The four questions within the survey captured the participants' gender allocation, age range, most used devices, and the daily hours spent surfing the Internet. 66.1% of the responses received were from the age group of 16-18 years old students. The female-male ratio was two-thirds of all responses while the gender dissemination of the age 16-18 year old group is more balanced with 57% female and 43% male students.

4.1.1 Students' Current Practices and Knowledge

The responses indicate that cell phones are the primary devices used by the students, with more than 74% of usage. Amount of daily Internet usage for 16-18 years old teenagers shows that about 30% of the students surf the web 5-10 hours per day, and a total of 30.8% of the students are online for more than 10 hours daily.

Table 2 summarizes the results of the students' knowledge in more detail. Based on this analysis, it can be concluded that the students lack knowledge of basic cyber security practices and online safety, and hence, they are vulnerable to different types of cyber attacks. For course design purposes, we concluded that thee focus should be on mobile phones, their related security and cyber hygiene.

4.1.2 Content to be Taught

Based on the analysis of the current level of knowledge and technology use, the designed program included the following topics: General concepts of phone security, Security of unknown links click in mobile application, Backups, VPN security, Password security, Unattended Devices, Antivirus applications, and Phishing attacks.

4.1.3 Culture of Education in Iran

We validated our analysis and obtained further information from the interview with a school principal. In accordance to the interviewee, despite the Covid-pandemic and shifting to remote online studies,

"majority of the classes were organized tradition ally", i.e., teacher-oriented teaching methods. However, new approaches to teaching with distance learning are emerging:

- Using Moodle to organize classes
- Recording a voice message or a video clip and sharing with the students through Whats App

Cybersecurity awareness topics	Results
clicking unknown links	5.7% of students click on the links without any hesitation.
backups	62.4% of students do not know how to backup and value of information on their devices.
VPN security	45% of students say they know entirely what VPN security is, or their knowledge is based on reading about it. The majority only know what VPNs are used for.
password security	majority of the responses showed that they use their names, birth dates, and phone numbers as their passwords as it was an easy-to-remember characteristic. However, the fact that some reported their passwords through the form was alarming.
abuse of the unattended	22% of students have not anything important or confidential to be exploited. In contrast, 35% specified that there is a possibility of their phones and social media being abused.
device phone antiviruses	17% of students know about phone antiviruses and have them installed on their phones. 31.9% of students think it is not an essential application. Meanwhile, 50% of them do not know that phone antiviruses exist, or do not know if installed on their devices.
software update	76.7% of students either have their automatic updates activated or update manually. A reason may be many screen pop-ups/notification when software update is requested.
phishing attacks	60% of students declared that they have never heard of this concept. Amongst the remaining respondents, only a few commented correctly on their understanding.
being hacked	92% of students have never been victims of a cyber-attack. It seems "yes" responders only consider financial or data theft-related attacks as cyber-attack.
cyberbullying	42.5% of students declared their familiarity with cyberbullying. Only 3.7% of students noted that they are aware of cyberbullying and had been a victim of it.

Table 2: Evaluation of students current knowledge.

- Uploading educational videos on Moodle
- For exams, video calls take place over Whats App that the teachers can ask students the questions
- Self-study methods involve teachers asking students to go through specific chapters of a book and contact them if they have any questions or need more clarification.

4.1.4 Online Environment

No physical face-to-face classes took place in Iran at the time of this research due to COVID restrictions. Hence, the best alternative for the live class room lecture-style teaching method were online class rooms through Skype, Zoom, Google Classroom, or other applications that provide a similar experience to interactive in-person classes.

4.1.5 Learning Outcomes

It is planned for the students to remember, understand and apply the discussed topics following the Bloom's Taxonomy (Krathwohl, 2010).

For the general concepts of cyber security, students will : understand the definition of cyber security and its importance demonstrate their understanding of phone security, and apply the actions discussed to increase their phone security. Related to security of unknown links in mobile application, students will: understand the ways to receive an unknown link action appropriately when receiving a link improve their differentiation between fake and genuine messages be introduced to the way they can check a short link, and apply the actions discussed to increase their phone security. For backups, students will: understand the definition of backups, their importance, and benefits identify the lack of it on their devices (if any) learn how to activate the backups for different applications, and implement the use of backups for their mobile de vices and applications. On VPN security topic, students will: understand the definition of VPN, its advantages and disadvantages identify trusted and untrusted VPNs using the introduced tools be given a list of trusted VPNs to install, and implement the tools when installing a new VPN. In password security, students will: acknowledge that if personal information is used in a password, it will be easy to guess identify a strong password from a weak password, and apply the tools when choosing a new password.

For unattended devices, students will: understand the risks of leaving their devices unattended be familiarized with some case studies of misusing unattended devices, and in the future not leave their devices unattended. In regards of antivirus applications, students will: understand the benefits of installing an antivirus be familiarized with trusted and most highly rated antiviruse applications, and use antivirus application on their devices. On phishing attacks topic, students will: understand what phishing attacks are identify measures to prevent a phishing attack be familiarized with some case studies of phishing attacks, and take actions to prevent such attacks.

4.1.6 Cultural Aspects of Analyse Phase

Our self-assessment of the three I's application in practice for this stage is as follows:

- Intention: We aim to design a culturally-sensitive program. We measure students' awareness level on different topics and obtain understanding of the cultural context. One of the findings of cultural aspects could be the absence of cyber bullying in social media amongst Hormozgan teenagers.
- Interaction: We interacted with students via survey, also school principal interview and interaction between the authors themselves.
- Introspection: We have authors both from Iran and West and the cultural aspects of the course design choices were discussed.

V. CONCLUSION

A cyberspace is now often more crowded than a physical space. With global pandemic, face-to-face experiences are even further reduced and many daily activities are now performed online. Unfortunately, the Internet users, including adolescents as shown in our survey for Iran's Hormozgan region, have low awareness of the dangers associated with online activities. Therefore, there is a need for cyber security experts, businesses, and schools to raise students' cyber security knowledge. Culture and education are inextricably linked in any well-designed program (Thomas et al., 2003). Thus, one of the attributes of a successful program is its level of engagement with the community it sup ports. This research followed and evaluated in practice the ADDIE instructional design model, using culture as the third dimension (Thomas et al., 2003) when implementing a CSA course for 16-18 years old high-school students.

The following are the main findings of this research:

- There are established cyber security training programs for Iranians but these focus on the business sector and employees. There are no published and evaluated initiatives designed for students and youth.
- Due to the differences in Eastern and Western cultures, there is need for a culturally-sensitive design criteria and Western-developed training courses may not be appropriate to Iranian society.
- We assessed the students' current CSA levels, using a quantitative survey method. Based on 616 responses, it can be concluded that students lack knowledge on basic cyber security principles.
- We have described the cultural and technological differences between Iran and Western countries relevant for CSA course design. The aspects to consider include e-mail usage, Internet censor ship and VPNs and Islamic culture. The designed course included topics that are not widely coveredin Western awareness courses, e.q., VPN security (which is widely used in Iran) and no extensive coverage on E-mail security (as irrelevant in Iranian high-school context).
- The ADDIE method with cultural embrace (Thomas et al., 2003) provides guidance on incorporating the three I's throughout the course life-cycle. However, from implementation perspective the guidance is high-level and practical use could be enhanced by providing the questions to self-assess the cultural aspects in each stage.

We piloted the course and evaluated the findings that showed students' overall improvement of knowledge and understanding on chosen cyber security topics. Further work should continue with a wider training audience to include high-school boys and considering cultural adjustments needed and also evaluating the results of the course in the longer time period to determine behavioural change. This study is a step in contributing to raising the students' awareness in Iran and to the science by practically implementing the ADDIE model with cultural embrace in cyber security awareness course design.

VI. REFERENCES

[1]. R. E. Beyer and B. J. Brummel, "Implementing effective cyber security training for end users of computer networks," SHRM-SIOP Sci. HR Ser. Promot. Evidence Based HR, 2015, [Online]. Available: https://www.shrm.org/hr-today/trends-and forecasting/special-reports-and-expert views/Documents/SHRM-SIOP Role of Human Resources in Cyber Security.pdf.

[2]. E. C. Controls, "Essential-Cybersecurity Controls," vol. 2018, 2018.

[3]. Euler Hermes, "Saudi Arabia Country Risk Report & Analysis," 2017, [Online]. Available: https://www.eulerhermes.com/en_CA/resources/country reports/Saudi Arabia.html#link_internal_1.

[4]. H. Tianfield, "Cyber Security Situational Awareness," Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom CPSCom-Smart Data 2016, pp. 782–787, 2017.

[5]. M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," J. Comput. Inf. Syst., 2020.

[6]. V. D. Andrews, "CSU ePress In-Depth Analysis of College Students ' Data Privacy Awareness," 2020.

[7]. W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, "Cybersecurity Awareness Level: The Case of Saudi Arabia University Students," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 3, pp. 276–281, 2021.

[8]. A. Garba, M. A. Musa, and S. H. Othman, "A Study on Cybersecurity Awareness Among Students in Yobe : A Quantitative," no. July, 2020.

[9]. E. M. Rogers, "17 - Rogers 1995 cap 6.pdf."p. 26, 1995.

[10]. T. Dinev and Q. Hu, "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," J. Assoc. Inf. Syst., vol. 8, no. 7, pp. 386–408, 2007.

[11]. C. Macabante, S. Wei, and D. Schuster, "Elements of Cyber-Cognitive Situation Awareness in Organizations," pp. 1624–1628, 2019.

[12]. M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," Hum. Error Aviat., vol. 37, no. March 1995, pp. 217–249, 2017.

[13]. "Copyright ©2000. All Rights Reserved.," 2000.

[14]. N. A. Stanton, P. R. G. Chambers, and J. Piggott, "Situational awareness and safety," Saf. Sci., vol. 39, no. 3, pp. 189–204, 2001.

[15]. F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," Int. J. Child Computer Interact., vol. 30, p. 100343, 2021.

Cite this article as :

N Satyanandam, Veldi Sriya, Cheripally Shravani, "Cyber Security Awareness in Online Education : A Case Study Analysis", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 4, pp. 55-61, July-August 2023.

Journal URL : https://ijsrset.com/IJSRSET23103159