

Culturally-sensitive Cybersecurity Awareness Program Design for Iranian High-school Students

Rooya Karimnia, Kaie Maennel^a and Mahtab Shahin^b
Tallinn University of Technology, Ehitajate tee 5, Tallinn, Estonia

Keywords: Cybersecurity, Cyber Awareness, Learning, Training, Cyber Hygiene, High-school, Students, Iran, Hormozgan.


Abstract: Many of our daily activities are performed online, which calls for everyone to learn more about cybersecurity. Designing a culturally-sensitive cybersecurity awareness course is essential to “speak” to training audiences with different cultural backgrounds and technology. We analyse the current cybersecurity awareness level of high-school students in Iran, Hormozgan, based on a survey of 616 responses. We develop an awareness program for 16 to 18-year-old students using the culturally-sensitive ADDIE model. We implement the program and evaluate its effectiveness by pre-and post-test methods. We also evaluate whether cultural aspects of Intention, Interaction, and Introspection are practical and sufficient in designing a cultural dimension to a cybersecurity awareness program. The key findings of the analysis show low cyber hygiene knowledge levels, excessive use of VPNs and that lectures are a preferred learning method. Based on practical application, we conclude that the ADDIE model with cultural embrace provides a means of incorporating culture into cybersecurity education. However, from a practical implementation perspective, the guidance is relatively high-level and would need further tailoring to focus on relevant aspects for cybersecurity training (e.g., technology use). The pre- and post-test results of a pilot session show increase in overall knowledge on selected cybersecurity topics.


1 INTRODUCTION

The majority of our daily activities such as communication, socializing, shopping, studying, and even voting are carried out using the Internet. Cyberspace provides us with opportunities and the means to establish communication through a range of different devices, regardless of geographical location. However, cyberspace includes also risks and threats, including malicious acts that seek to damage or steal data or disrupt our digital lives (Ghosh, 2020). Nowadays, due to the rise of distance learning, students extensively use the Internet to attend their classes, complete their assignments, and perform their exams in addition to their free time activities. We cannot simply expect users to understand existing risks and react to them appropriately, without some form of guidance (Korovessis et al., 2017). While awareness seeks to focus an individual’s attention on the issues, training seeks to teach skills (Korovessis et al., 2017). Training can make difference when aiming to safeguard a person’s

privacy and online security.

Therefore, there is a need for effective awareness and training programs about the online risks, prevention methods, and actions to be taken when facing hazards in cyberspace. Cybersecurity covers several areas, including tools, guidelines, and best practices. These aim to ensure the safety and security of the cyber environment and user’s assets such as devices, applications, services, and the totality of transmitted and stored information (Von Solms and Van Niekerk, 2013). Many cybersecurity awareness (CSA) trainings have been developed worldwide. However, the effectiveness of systems may be reduced where these are transferred into cultures for which they were not designed as suggested by theories of learning and cultural difference (Dunn and Marinetti, 2007). Effective training incorporates cultural understanding and therefore implementing a program developed for the Western culture cannot be assumed to be effective or relevant in Eastern or Islamic cultures. For example, the culture of wearing a Hijab in Iran necessitates a focus on secure storage of personal photos on their devices, while in other cultures people publish per-

^a  <https://orcid.org/0000-0002-3886-9532>

^b  <https://orcid.org/0000-0002-5784-6301>

sonal pictures without a second thought. We follow this epistemology of cultural sensitivity when choosing and applying research aims and methodology in this research.

We analysed the current CSA level of high-school students in Iran, Hormozgan and developed a CSA program using culturally-sensitive ADDIE model (Thomas et al., 2003). We also implemented the proposed program and evaluated its effectiveness by using a pre-and post-test method. During this process we evaluated whether cultural aspects of Intention, Interaction, and Introspection (Thomas et al., 2003) aspects are practical and sufficient for including cultural dimension to a CSA training program.

Our main contributions include the development of a methodology and assessment of the current Hormozgan high-school students CSA level based on 616 responses. These survey findings could be used as a starting for future research in other states of Iran. We added cultural sensitivity aspects as part of the development and evaluation of a CSA course specifically designed for Iranian high-school students. We evaluate and share the practical implications when adopting the culturally-sensitive ADDIE model (Thomas et al., 2003) to address the cultural sensitivity and technology use in the CSA programs.

2 BACKGROUND AND RELATED WORK

2.1 CSA Programs around the World

Awareness programs aim to teach individuals to recognize IT security concerns and respond accordingly (Paulsen and Byers, 2019). Several studies have been performed on CSA level of different student groups globally, e.g., (Tirumala et al., 2016). When developing CSA courses, the variety of designs and content is covered, such as (Das et al., 2017), (Mccoy and Fowler, 2004) and (Cai and Arney, 2017). However, results have shown that middle school students are the least responsive to a CSA training, as they do not comprehend how stolen information can have life-impacting consequences (Smith and Ali, 2019). Overall, the focus is on the content and effectiveness of delivery, and the cultural aspects are rather implicit and not necessarily directly discussed.

2.2 Cybersecurity Awareness in Iran

In Iran, advertising the importance of cybersecurity is a relatively new initiative despite 81.5% of Irani-

ans are using the Internet¹. There are only few online courses in Persian language, which mostly focus on employees' awareness, e.g., (Nozari, 2021), (Heydari, 2020), (Ghahrood, 2019) and (Samouti et al., 2019). There is not much cybersecurity training for the school students. However, to date, there is not much research conducted on developing a well-structured CSA program in Iran (Samouti et al., 2019). A workshop held by the Iranian Police to female high-school students in Razavi Khorasan State² is the only case where public information has been found. However, there is no scientific evaluation and it is for a different state. In high-school curricula there is only one computer course "Basics of Computer and Informatics". This course is only taught in the third year and to those who have selected Math and Physics as their high school majors (note: 3 majors are Maths and Physics, Literature, and Experimental Sciences)³. This information illustrates that the students knowledge of computers is relatively low. It also indicates that schools do not prepare students to protect themselves against the dangers of virtual world.

2.2.1 Influence of Culture on Cybersecurity Practices and Values

Culture is a set of traditions moulded by religion, ethnicity, language, and history (Garrett, 2004). Culture serves as a lens through which a society views the world. With the Internet and new communication technologies, the communities, way of living, cultures, values, and even family relations are affected. However, depending on the beliefs and the freedom given to people of any culture, these changes may take effect or be discarded by the community. In Iran, many discussion subjects are prohibited, such as sensual topics (Shah Ghasemi, 1985). The changes brought to Iran's culture through technological advancement are undeniable. However, the authorities see that they need to control new changes, and only those in harmony with the ruling government's goals are allowed (Karimi Zadeh et al., 2015). The CSA programs promote a change in behaviour and attitudes. Therefore, society and its organisations, including schools, should provide awareness approaches that combine training with culturally-sensitive cybersecurity policies and education.

¹<https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/>

²<http://spooler.ir/1395/09/1407/>

³<http://www.kashiha.ir/list/daberestan/{1th,2th,3th}.htm>

2.2.2 Cultural Aspects for CSA Programs in Iran

The cultural aspects that are integral with Iranian culture need to be considered when designing cybersecurity training for Iran. A failure to do so would reduce the course effectiveness. The aspects to consider are:

- **Islamic Hijab Culture**—The hijab plays a major role in the lives of most Iranians. Unfortunately, it is common for incidents such as leakage of the Hijab-less photos occurring, which can have a detrimental effect on family relations.
- **Censorship and VPN**—Due to the Internet censorship in Iran, people tend to use VPNs regularly to access content (Aryan et al., 2013). If the VPN is not downloaded from a benign source, it could lack encryption and lead to traffic leaks, contain malware, allow a third-party to track and access sensitive phone permissions or cause other compromises on the security of the devices (Ikram et al., 2016).
- **Tools Usage**—Among students in Iran, the use of emails is minimal and they tend to download media from a range of sources rather than checking their emails (Tajik Ismaili and Yousef Zadeh, 2016). When teaching students about clicking unknown links, the role of media downloads could be used as an example.
- **Limited English Language Skills**—Hormozgan students lack English proficiency (Zarrabi and Brown, 2017) and thus there is possibility that they could develop a habit of clicking on any button they see on the screen when a pop-up message appears, without actually understanding the consequences of clicking (Rana, 2012).
- **Lack of Free Public WiFi**—Public WiFi connection is an essential topic in the CSA courses developed in the US and the EU, however this is irrelevant in Iran as typically no free WiFi⁴.
- **Lack of Browser Cookies**—None of the major Iranian websites have cookie usage agreement pop-up displayed⁵ and thus the overall understanding on this topic is low.

2.2.3 Iran and Hormozgan Province

Hormozgan is located in southern Iran. In general, the people there speak different dialects from Persian. However, children learn Persian from an early age because it is the medium of communication in

⁴Mastkin, A. and Ghiasi, A. Free Public Internet; Reality or a Dream? <https://digiato.com/article/2017/10/28/>

⁵Tahmasebi, V. What Are the Best Iranian Sites, <https://karsazsho.com/what-are-the-best-iranian-sites>

schools⁶. Hormozgan is one of the most deprived states of Iran (Rana, 2012). Searching through English and Persian literature, at present there is no research published on Hormozgan’s students knowledge and awareness on any topic, including cybersecurity.

3 METHODOLOGY

There are many different instructional design models, such as Gagne’s Nine Events of Instruction (Gagne et al., 2005), Merrill’s Principles of Instruction (Merrill, 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).

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

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

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 va-

⁶https://en.wikipedia.org/wiki/Hormozgan_Province

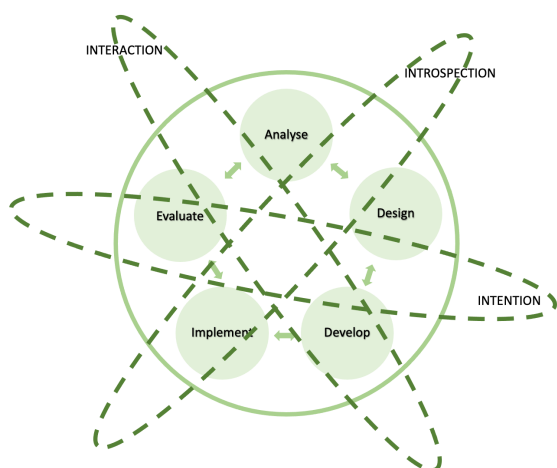


Figure 1: ADDIE model with culture elements (Thomas et al., 2003).

lidity of the research. As the main methods in Analyse step, a quantitative survey and interviews were conducted. In Evaluate step pre-and post-test approach was instrumented. More details about methods applied are described in Section 4.

4 IMPLEMENTATION AND RESULTS

4.1 Analyse

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 ensure impartiality and validity of research.

The questionnaire captures the students' existing knowledge on the CSA topics following the main cy-

⁷<https://knoema.com/atlas/Iran/Hormozgan>

bersecurity threats in Iran (Shoja Heydari, 2015), including clicking unknown links, backups, VPN security, password security, abuse of the unattended device, phone anti-viruses, software updates, phishing attacks, being hacked and cyberbullying.

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 cellphones 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 cybersecurity practices and online safety, and hence, they are vulnerable to different types of cyber attacks. For course design purposes, we concluded that the 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 traditionally", 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 WhatsApp

Table 2: Evaluation of students current knowledge.

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.

- Uploading educational videos on Moodle
- For exams, video calls take place over WhatsApp 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 classroom lecture-style teaching method were online classrooms 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 cybersecurity, students will:

- understand the definition of cybersecurity 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 devices 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 cyberbullying 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.

4.2 Design

The program design focus on the development of a culturally-sensitive course that provides students with information, skills, and encouragement to apply basic cybersecurity concepts. To ensure that the learning aims are achieved and measurable, Bloom's taxonomy has been considered to provide the students with the Apply level skills (Krathwohl, 2010).

4.2.1 General Program Description

The course is called "Introduction to Cyberspace Security" and is taught to 16 to 18 years old high-school students in Iran, Hormozgan. The program is completed in two sessions of 1.5 hours each and designed for a class of 20 students to ensure sufficient teacher-student interaction. The medium of the instruction is

Persian, and the class is organized using the BigBlue-Button⁸ tool. The students are able to register for the class by contacting authorities in the schools they are enrolled in. The overall course aim is an increase in the students' awareness level and provide them with the knowledge and skills to apply the concepts learned within this course in daily online activities.

4.2.2 Tools for Students' Engagement

Slides were used as visual learning aid. Also to reinforce and measure the learning impact pre-and post-test questions were distributed.

One of the instructional challenges in online classrooms is achieving high levels of interaction (Jacobs, 2013). This means that innovative techniques and various resources should be used in the learning process (Jacobs, 2013). These include online tools such as Wooclap⁹ and gamification. Wooclap is used for asking questions addressed to all the students, instead of asking for volunteers to speak. In this way many attendees may have the courage to type their thoughts. As a gamification element, a game of Guessing Password is planned. More details on the game can be found in Section 4.3.1.

4.2.3 Course Outline

To capture the students' attention, the method of storytelling is used. This has been introduced as an effective way of teaching in which students' attention would be caught at first and followed by an item to remember when thinking of the class events (Blaustone, 1991). As a result, a relevant and adequately alarming story about the hijab-less pictures being stolen and used for blackmail is told to relate the topic to students and attract their attention.

Lecture 1. This lecture contains basic definitions and information on the definition of cybersecurity, its importance and principles, aiming to reach the Apply level of Bloom's taxonomy. By the end of session, it is expected that students have basic knowledge on the content discussed and motivation to use the information gained for applying security in their daily lives.

Lecture 2. This lecture aims to ensure that students have sufficient information and are aware of the consequences of leaving their devices unattended and failing to back up their data. This session also addresses the value of antivirus applications and backups while ensuring that students understand how to

⁸<https://bigbluebutton.org>

⁹<https://www.wooclap.com>

install and activate them. Consequently, it ensures that they have a general understanding of actions to take if they have been hacked. By the end of session, it is expected that students use the knowledge to increase the security of their devices, meeting the apply level of Bloom's taxonomy.

4.2.4 Evaluation Method

The pre-and post-test approach is a commonly accepted way to assess the instructional program's effectiveness (Felix, 2016). When majority of the students respond to both tests, a baseline can be established for comparison (Felix, 2016). In addition to the pre-and post-test, two questions are posed during the class that are useful both for learning retention and evaluation. The first question is posed at the beginning of lesson, asking students to rate their current cybersecurity knowledge on a scale of one to one hundred. The second question is asked at the end of lesson, in which they give another appraisal of their knowledge and to name one thing they have learned.

4.2.5 Cultural Aspects of Design Phase

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

- **Intention:** We aim to design a culturally-sensitive program. We recognise that there are some taboo topics (such as sexual content) discussed in Section 2.2.2. For example, sextortion¹⁰ cannot be directly covered but in a way is very relevant due to hijab culture and privacy.
- **Interaction:** In regular communication between authors both from Iran and West, we discussed what learning designs would work, etc. Also appropriate authority reviews and approvals need to be obtained, for example, the authors interacted with the school principal directly to validate the program's material.
- **Introspection:** We were tempted to adopt the tools from the West, however the choice of learning tools in instructional design also needed to consider cultural aspects. For example, Wooclap and many other similar online tools are in English language and using cookies. However, Iranians when surfing Iranian sites are not familiar with seeing cookies and agreement pop-ups. Therefore, a small tutorial is needed to familiarise with the Wooclap website and inform students about need to read the agreement before agreeing to pop-up

¹⁰<https://dictionary.cambridge.org/dictionary/english/sextortion>

terms and conditions. At the same time this is a practical activity about external websites.

4.3 Develop

Main development stage activities include the content slides and pre-and post-tests development for learning reinforcement and evaluation.

4.3.1 Session Plan

A total of 28 content slides were prepared in Persian for the two sessions. The first slide is for introducing the lecturer, followed by a cybersecurity incident affecting a 19-year-old girl in Iran. A real-life story talked about how the girl's phone was hacked in a gathering and the consequences she had to face due to the incident¹¹.

The next slide focuses on defining cybersecurity and reasons of its importance, followed by the interactive question that asked students to visit the link and rate their current cybersecurity knowledge. The following slide demonstrates that the course focuses on phone and tablet cybersecurity-related issues only with a summary of the course outline: Phone Security, VPN Security, and Unknown Link Clicks. Afterwards, four items on the importance of phone security were specified. For instance, storing personal information such as family photos and chats and logging into social platforms, particularly Instagram using phones, are reasons to be aware of phone security.

The session continues with a focus on phone security principles starting with sharing a Wooclap link with the students, asking their opinion on what can be done to increase our phone security. Subsequently, few general guidelines such as activate "Find my phone" on phones and instruction on remote phone formatting were provided. Additionally, several trusted antivirus applications are shared with the students.

VPN security is the topic to be discussed. A general concept of what VPN is, how it works, and its advantages and disadvantages are addressed. To ensure the Apply level of Bloom's taxonomy is met, two websites are introduced to test the VPNs' security. The websites used are <https://whatismyipaddress.com/> and <https://dnsleaktest.com/>. During the initial stage of this research, one of the survey questions was, "In case you are using VPN for specific applications, please specify them here." Interestingly, some of the students responded to this question with the VPN

¹¹Destruction of the young lady's life through her hacked phone, <https://persianv.com/havadets/>

application's name. All the VPNs mentioned in survey were tested against the websites mentioned earlier. Unfortunately, many of the VPNs were not secure. Amongst those, Vpnify and Star VPN were selected to demonstrate secure and unsecured VPNs. The students were asked to switch on the installed VPN and check the websites. Later on, they are introduced to a few reliable VPNs and encouraged to install in order to improve their security.

The third topic discussed was the dangers of clicking on unknown links. The aim was encouraging students to stop, read and think before they click. An example shared was presenting two SMS messages, and asking students to guess which of the links are actual and fake. To help differentiating between a fake and an original link, they are introduced to Google's Transparency Report platform (Google, 2021). Students are requested to check the received link on this platform before tapping on the link. Apart from this, students are familiarised with the types of links, short and long URLs, and the ways they can identify and check the legitimacy of redirected websites.

The next topic is password security. Password Guessing Game is played by asking for one volunteer. A volunteer was asked some basic questions such as birthday and phone number while the trainer would attempt to guess the password. Moreover, students are familiarised with <https://haveibeenpwned.com/Passwords> website to test the phrases they have in mind before password selection and advised to change their passwords immediately if they are compromised.

Towards the end of class, a summary of the course is provided so that revision of its content can be studied. Finally, another Wooclap link is shared, asking students to name an item they have learned and giving their cybersecurity knowledge another rating.

4.3.2 Pre-and Post-test

To measure the learning impact, the pre-and post-test were prepared. The first two questions of the pre-test are to measure the students' knowledge of phone security so that it can be compared to the post-test results. Questions 3-4 focus on password security, aiming to understand students' approaches towards passwords selection. Questions 5-6 record the awareness of VPN security, and the last one aims to grasp their current practices when receiving an unknown link. The post-test questions follow the same flow as the pre-test. Furthermore, we used two interactive questions during the session to understand how knowledgeable students see themselves in cybersecurity and to reinforce their reflection of the subject matter.

4.3.3 Cultural Aspects of Develop Phase

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

- **Intention:** We aim develop the course, slides, and pre-and post-test questions in context to Iranian culture, specifically focusing to students' online activities. For example, we discarded topics such as Public WiFi Connections, and E-mail Security, while focused on topics like VPN Security.
- **Interaction:** We were requested to run a pre-pilot version for the principal and two other teachers due to the lecture being originated from a Western country.
- **Introspection:** As a result of pre-pilot the authors were asked to wear Hijab in an Iranian class and a picture displayed on slide deck (which showed a female's skin) was requested to be changed, however no changes were made to the awareness topics planned and delivery style. This was strong reminder of the cultural aspects being important at very detailed level. Also in regards of authors' differing experiences on teaching methods, we discussed and decided to retain the interactivity feature, although it is not well practised in Iranian education system.

4.4 Implement

We implemented a delivery of the designed CSA program to validate the effectiveness of design and appropriateness of cultural fit. Due to the time limits and COVID restrictions, the program was delivered to one high-school class in Hormozgan. As the schools in Iran are single-sex, a female class of 27 high school girls aged 17 years old was selected. The school's Moodle platform¹² was used for delivery.

The session started by introducing the lectures, and the developed content was used to deliver the training. Some highlights from the session as were follows:

- When requesting the students to reply on how to increase phone security, half of the responders mentioned setting a solid passcode for phones as the best way to enhance phone security.
- When the students were asked to guess which of the SMSs shown is real and fake, 48% selected correct answer as the real SMS, whereas the incorrect choice represented an actual SMS message from the advertising company.
- When the Password Guessing Game was played,

¹²<https://lms.sultanolama.com>

the volunteer student Zahra¹³ disclosed information that she was born in 4, Mehr 1383 and 0996 to be the last four digits of her phone number¹⁴. The trainer then guessed her password to be Zahra83, and she innocently revealed other information, such as the previous phone number she owned ended with 38, and the password also contains some symbols. Then the trainer again guessed 38*Zahra*83 or 38!Zahra!83 or 38@Zahra@83. She agreed that the first password is very close to her correct password. This game acted as a warning call for many of the students based on the post-test results.

In addition, the day before scheduled class the school principal distributed the pre-test amongst students and total of 27 responses were collected. The post-test was shared after the class, and a total of 23 responses were collected.

4.4.1 Cultural Aspects of Implement Phase

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

- **Intention:** We deliver the course in coherence with the societal norms of Iran and in alignment of the cultural changes requested in earlier stages.
- **Interaction:** We achieved interaction during the session delivery and the feedback collected from the students.
- **Introspection:** We reflected on the delivery experience. Overall, the structure of online classes is very similar everywhere around the world. However, some infrastructural issues such as access to the Internet or not having a smart-phone affected online training for two students.

4.5 Evaluate

Within this section, the results of the pilot delivery are discussed. Despite the fact that only one class was held, the efficacy of CSA program was assessed using the two criteria. Firstly, distribution of pre-and post-test and comparing students gained knowledge and secondly, using the two Wooclap links to rank students confidence on cybersecurity concepts before and after the class.

¹³note that the volunteer's name is changed to protect her privacy, however known to the authors

¹⁴for more information on converting Jalali Calendar to Gregorian dates, see wikipedia.org and HoomanB.com

4.5.1 Pre-test and Post-test Results

The pre-and post-test results are summarised in Table 3, which show an increase of correct answers in all topics. One of the finding was that during pre-test 47.7% of the students selected a combination of their name, birth date, and phone number to describe their current passwords. When the same question was asked during the post-test, no student mentioned that they had selected personal details as passwords.

Table 3: Pre-test and Post-test Results.

Topic	Pre-test	Correct answers	Post-test	Correct answers
Phone security	1	77.7%	1	95.8%
Phone security	2	62.9%	2	65.2%
Password security	3	39.2%	3	91.3%
Password security	4	62.9%	4	95.6%
VPN security	5	22.2%	5	82.6%
VPN security	6	14.8%	6	52.2%
Unknown links	7	81.5%	7	95.6%

4.5.2 In-class Wooclap Results

Wooclap links shared at the beginning and end of the class asking students to rate their cybersecurity knowledge were analysed. At the start, the responses had a mean of 23.27 on the percentage of their current cybersecurity knowledge based on their judgement. However, the average of their knowledge increased at the end of session. Students ranked their knowledge with an average of 58.75, also stated the following:

- I moved from 25% to 50%. Tips on differentiating fake and real links.
- Everything was new to me.
- I learned about using a trusted VPN, think before click, and check my password first and making sure it is strong enough. (2x)
- I learned that when using an application or clicking on a link, we have to consider the possibility of allowing a hacker to access our data.
- I will start today implementing what I have learned.
- I did not know using VPNs had side effects, and I always used my name and birth date for my password. I will not use this information in my passwords ever again.

Figure 2 illustrates the relation between achieved goals of each topic and their correspondence to Bloom's taxonomy.

In summary, the pre-and post-test responses combined with the information gathered on the students' confidence levels, were analysed. Although only one

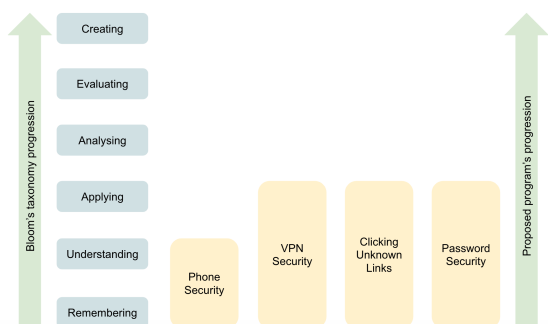


Figure 2: The course progression and its correspondence to Bloom's taxonomy.

pilot class was implemented, the results were promising. These showed an increase in awareness and motivation to apply and use the tools shared in their daily online interactions.

4.5.3 Cultural Aspects of Evaluate Phase

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

- **Intention:** We aim to evaluate the success and effectiveness of the course with respect to cultural values of Hormozgan state.
- **Interaction:** We interacted between the authors while performing evaluation, but also with the student who revealed her personal data. We also communicated with the other Iranian school teachers, who showed interest in a similar course.
- **Introspection:** We reflected on the evaluation experience whether the pre-and post-test results are indicative of the appropriate cultural aspects, and how the course can be further improved or adopted for the different audience (e.g., would the same opening story work for class of 16-18 boys or needs to adapted or changed).

5 DISCUSSION INCLUDING LIMITATIONS, ETHICS AND PRIVACY

5.1 Discussion

Culture plays an important role in education, and therefore the training content and the process of organizing class are distinct in Iran. We have described the three I's (Intention, Interaction, and Introspection) and cultural aspects in each stage of the ADDIE model, see Sections 4.1.6, 4.2.5, 4.3.3, 4.4.1, and 4.5.3.

Our research contributes academically by implementing the ADDIE model with cultural embrace by (Thomas et al., 2003) for a CSA course and evaluating its usability and practical aspects of implementation. The model is straightforward and introduces the three I's as providing cultural context. However, it was not as practical as expected because the concepts and guidance stays at high level. It would be practical to develop a check-list or similar tool to provoke the thoughts for each stage and for each of the three I's. We experienced that within the first three stages of the ADDIE model (Analyse, Design, and Develop), the three I's provided very helpful and different angles. However, for the last two stages of the ADDIE model (Implement and Evaluate), the cultural aspects became more apparent and significant. This suggests that the methodology could be further revised so that the three I's have particularly high focus on the Analyse, Design, and Develop stages of the ADDIE model.

Also a question may arise, why develop a new course and not just adopt an existing western CSA course for Iranian culture or another course in Persian language to high school students? Firstly, we wanted to put the ADDIE model with cultural embrace into practice (Thomas et al., 2003) as we have not found any practical evaluation of this model for cybersecurity. While cultural considerations are similar in other existing Persian cybersecurity training courses, these are unfortunately either the too generic or targeting employees that requires more compliance focus. Therefore, we concluded that developing a new training focusing on cultural elements and based on the relevant topics identified in Analyse phase is appropriate.

5.2 Limitations

The authors recognise that there was only one pilot class and in order to evaluate the effectiveness further course deliveries are needed with larger sample size in order to be representative for Hormozgan student population. However, the pre-and post-test results of the pilot class are indicative for a positive impact. Additionally, it is important to note that the long-term effects of the designed course cannot be measured at the time of completion of this study. Since the aim of this paper is to measure and increase the awareness level of high school students in Iran, Hormozgan, no initiative has been taken so far to measure the behavioural changes of the students. This means that a longitudinal study is needed to measure the behaviour change such as using the secure password and not connecting to an untrusted VPN.

5.3 Ethics and Privacy

This research focused on students who are mainly under 18, i.e., they are legally under-age. Therefore, it was critical to address the ethical and privacy issues raised by any information exchanged. When preparing the questionnaire and pre-and post-test questions, special care was taken to ensure that no personal information was accessed and that the answers were collected anonymously. Also, the authors contacted the student who revealed her password via WhatsApp immediately after class and was advised to change her password on all her platforms. Also, throughout the development process we focused on the culturally sensitive design that follows Iranian ethical norms. It is also worth noting that the planned material was double-checked with school officials to ensure that it is appropriate for the students.

6 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 cybersecurity experts, businesses, and schools to raise students' cybersecurity 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 supports. 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 cybersecurity training programs for Iranians but these focus on the business sector and employees. There is 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 cybersecurity 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 censorship and VPNs and Islamic culture. The designed course included topics that are not widely covered in Western awareness courses, e.g., 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 cybersecurity 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 cybersecurity awareness course design.

REFERENCES

- Aryan, S., Aryan, H., and Halderman, J. A. (2013). Internet Censorship in Iran: A First Look. Technical report.
- Blaustone, B. (1991). Teaching Evidence: Storytelling in the Classroom. *American University Law Review*, 41.
- Cai, Y. and Arney, T. (2017). Cybersecurity should be taught top-down and case-driven. In *Proceedings of the 18th Annual Conference on Information Technology Education*, pages 103–108. ACM.
- Campbell, P. C. (2014). Modifying ADDIE: Incorporating new technologies in library instruction. *Public Services Quarterly*, 10(2):138–149.
- Das, A., Voorhees, D., Choi, C., and Landwehr, C. E. (2017). Cybersecurity for future presidents: An interdisciplinary non-majors course. In *Proceedings of the Conference on Integrating Technology into Computer Science Education*, pages 141–146, New York, USA. ACM.
- Dunn, P. and Marinetti, A. (2007). Beyond localization: Effective learning strategies for cross-cultural e-learning. In *Globalized e-learning cultural challenges*, pages 255–266. IGI Global.

- Felix, A. (2016). Using pre/post-testing to evaluate the effectiveness of online language programs. *Journal of Second Language Teaching & Research*, 4(1):176–193.
- Gagne, R. M., Wager, W. W., Golas, K. C., Keller, J. M., and Russell, J. D. (2005). Principles of instructional design.
- Garrett, C. (2004). Developing a security-awareness culture—improving security decision making. *SANS Institute InfoSec Reading Room*.
- Ghahrood, A. (2019). Raising cyber security awareness (internet security).
- Ghosh, K. (2020). Identification and quantification of cybersecurity risk by likelihood-severity, incident-response and organizational asset valuation framework. *Incident-Response and Organizational Asset Valuation Framework*.
- Google (2021). Google Safe Browsing – Google Transparency Report.
- Heydari, M. (2020). Teaching Cyber Security.
- Hill, R. (1998). What sample size is “enough” in internet survey research. *Interpersonal Computing and Technology: An electronic journal for the 21st century*, 6(3-4):1–12.
- Ikrum, M., Vallina-Rodriguez, N., Seneviratne, S., Kaafar, M. A., and Paxson, V. (2016). An analysis of the privacy and security risks of android vpn permission-enabled apps. In *Proceedings of the 2016 Internet Measurement Conference*, New York, USA. ACM.
- Jacobs, P. (2013). The challenges of online courses for the instructor. *DigitalCommons@SHU: Criminal Justice Faculty Publications*.
- Karimi Zadeh, M. M., Rafi Zade, E., and Kholgh Nik, D. (2015). A study on the connection between culture and virtual space and presenting solutions for. In *1st National Conference on Cyber Space and Cultrual Changes (CSCC 2015)*.
- Korovessis, P., Furnell, S., Papadaki, M., and Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. *Journal of Cybersecurity Education, Research and Practice*, 2017(2):5.
- Krathwohl, D. R. (2010). Theory Into Practice A Revision of Bloom’s Taxonomy: An Overview. *Theory Into Practice*, 41(4):212–218.
- Mccoy, C. and Fowler, R. T. (2004). “You Are the Key to Security”: Establishing a Successful Security Awareness Program. In *Proceedings of the 32nd annual ACM SIGUCCS conference on User services*, New York, USA. ACM.
- Merrill, M. D. (2002). First principles of instruction. *Educational technology research and development*, 50(3):43–59.
- Nozari, A. (2021). Introduction to Cyber Security.
- Paulsen, C. and Byers, R. (2019). Glossary of Key Information Security Terms. Technical report, National Institute of Standards and Technology (NIST).
- Rana, S. B. (2012). SID.ir — Identifying deprived regions of Iran by Composite Ranking. *Research and Urban Planning*, 2(7):53–70.
- Samouti, S. A., Fathy, M., and Mohesen, A. (2019). A Survey on SAT Cyber Security Awareness Implementation Methods for Managing IT Security. In *10th International Conference on Information Technology and Knowledge*.
- Shah Ghasemi, E. (1985). A Revision on the Effects of Virtual Environment on Communication Views. *Global Media Journal*, (2).
- Shoja Heydari, B. (2015). Investigating the harms of the internet on adolescents and providing preventive solutions. In *Third International Conference on Recent innovations in Psychology, Counseling and Behavioral Sciences*.
- Smith, D. T. and Ali, A. I. (2019). You’ve been hacked: A technique for raising cyber security awareness. *Issues in Information Systems*, 20(1):186–194.
- Tajik Ismaili, S. and Yousef Zadeh, M. (2016). Investigating the relationship between the amount and type of Internet use and lifestyle. *Institute of Humanities and Cultural Studies*, 107(2).
- Thomas, M., Mitchell, M., and Joseph, R. (2003). The third dimension of addie. *TechTrends*, 46(2).
- Tirumala, S. S., Sarrafzadeh, A., and Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust*, pages 223–228. IEEE.
- Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38:97–102.
- Zarrabi, F. and Brown, J. (2017). English language teaching and learning analysis in iran. *International Journal of Educational and Pedagogical Sciences*, 9(10):3485–3493.