TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

Rooya Karimnia 194277IVCM

Culturally-Sensitive Instructional Design of a Cybersecurity Awareness Program for High School Students in Iran, Hormozgan

Master Thesis

Supervisor
Kaie Maennel

Co-supervisor
Mahtab Shahin

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Rooya Karimnia ....

(signature)

Date: April 22, 2021

Annotatsioon

Me elame maailmas, kus enamik meie igapäevaseid tegevusi, nagu suhtlemine, lävimine, ostlemine, õppimine ja isegi hääletamine, toimub veebis. Tulenevalt interneti olulisest tavaelus, on vajalik kõikide kasutajate, sealhulgas teismeliste, kuberturvalisuse alaste teadmiste parandamine. Iraanis on inglise keele oskuse ja kuberturvalisuse alase koolituse puudumise tõttu turvateadlikkus lääneriikidega võrreldes madalam. Käesoleva uurimustöö raames viidi läbi kusitlus Iraani Hormozgani provintsi keskkooliõpilaste õpilaste kuberteadlikkuse taseme analüüsimiseks. Kusitluse tulemuste alusel töötati välja ja viidi läbi kultuuriliselt tõhus kuberturvalisuse teadlikkuse kursus. Eesmärgi saavutamiseks on kasutatud ADDIE mudelit, mida on täiendatud kultuuri kui kolmanda mõõtmega [1]. Töö üheks eesmärgiks on selle metoodika testimine ja hinnata kuidas prakitikas kaasata kultuuriaspektid mudeli igasse sammu küberturvalisuse koolituse välja töötamisel.

Koolituse fookusgrupiks on Hormozgani osariigi 16-18-aastased õpilased. Esimese uuringu sammuna koguti kusimustiku abil teavet õpilaste teadmiste taseme kohta. Iraani Hormozgani õpilastelt saadi kokku 616 vastust. Tulemused sisaldavad sellist teavet nagu VPN-i madal turvalisuse tase ja eelistatud õppemeetod loengute läbiviimiseks. Seejärel on tehtud intervjuu gumnaasiumi direktoriga, et saada lisateavet nende kooli kultuuri õpetamise kohta. Kuigi uuringust ja intervjuust kogutud teave on piiratud ja seda ei saa uldistada, on saadud teave toetav kursuse disanimiseks. Nende sisendite alusel on koostatud kursus, kasutades Iraani kultuuriliste aspektide kohta saadud uksikasju. Näide kultuurilisest aspektist on Hijabi kandmise kultuur Iraanis ja seetõttu seadmetesse salvestatud fotode eriline tähtsus [2].

Kursuse väljatöötamisel ja läbiviimisel oli eesmärgiks, et tunni sisu ja korraldusmeetod saavutaksid Bloomi taksonoomia rakendamise taseme [3]. Koolitusprogrammi pilootversioon viidi läbi 20 õpilasega tüdrukuteklassile, mille käigus hinnati programmi efektiivsust eel- ja järeltesti meetodi abil. Pilootiprogrammi tulemused näitavad, et programm osutus tõhusaks. See suurendas edukalt proovitunnis käivate õpilaste kuberturvalisuse alaseid teadmisi ja motiveeris neid juhiseid järgima. Õpilastelt saadud tagasisides hinnati klassis kultuuri arvestamist, näiteks toodi välja hidžabita fotode seadmetessekinnitamise tähtsus.

Käesoleva töö raames viidi läbi väljatöötatud koolituse pilootprogramm, laiaulatuselikuma tulemuslikkuse hindamiseks on vajalikud edaspidised koolituste efektiivsuse ja kultuuriliste aspektide saavutamise hindamised suurema elanikkonna ja vastassugupoole seas.

Abstract

We live in a world that most of our daily activities, such as communication, socializing, shopping, studying, and even voting, are performed online. This excessive use of the Internet draws attention to the need for everyone, including teens, to learn more about cybersecurity. Security awareness in Iran is much lower than in Western countries due to a lack of English language skills and cybersecurity training in schools. This study aims to assess students' current levels of cybersecurity knowledge, as well as to establish and implement a culturally effective cybersecurity awareness course for old Hormozgan high school students aged 16 to 18. The ADDIE model with an additional third dimension of culture is used [1]. This choice was made to put this technique to the test and bring culture into every step of the process. A questionnaire is used to collect information on students' awareness levels at first. The students of Hormozgan, Iran, provided a total of 616 answers. Excessive use of VPNs and the preferred learning method of the students to be lectured are among the results. Then, an interview is conducted with a high school principal to obtain additional information on teaching culture in their school. Although the information gathered from the survey and interview is limited and cannot be generalized, the information gained is reliable. Additionally, a course is designed utilizing details obtained concerning the cultural aspects of Iran. An example of a cultural aspect is the culture of wearing a Hijab in Iran and, therefore, the particular importance of photos stored on devices [2].

Further, upon the development and execution of the course, it is ensured that the content and method of organizing class achieve the goal of reaching Bloom's taxonomy's Apply standard [3]. Only one pilot class is carried out for a class of girls-only containing 20 students. Future works focus on testing the program on a larger population and the opposite gender. The effectiveness of the program is measured using the pre-test and post-test methods and results suggested that the executed program is proven to be effective. The training successfully increased the cybersecurity knowledge of the students attending the trial class and motivated them to follow the guidelines. Feedback received from the students appreciated the consideration of culture in the class, such as pointing out the importance of securing Hijab-less photos in devices.

Table of Contents

List of Figures

List of Tables

1. Introduction

Whenever the topic cyberspace is discussed, people often think about the computers connected to the Internet, while computers are just a small fraction of the cyber world. The virtual world contains the majority of our daily activities such as communication, socializing, shopping, studying, and even voting. In other words, the Internet has become an inseparable element of our daily lives. Cyberspace provide us with the means to establish communication through different devices, regardless of geographical location.

Teenagers are not different from adults; in fact, they are spending more hours on the Internet daily as compared to elder ones [4]. Nowadays, due to the rise of distance learning in schools, students not only spend their free time surfing the world wide web, but also use the Internet to attend their classes, complete their assignments, and perform their exams. Therefore, in terms of education, the Internet is very useful as it furnishes the students with the knowledge they need to enhance their education and communication. On the other hand, significant dependency and usage of Internet has its risks. A comprehensive study on the online risks for teenagers suggested that the main risks teenagers face online are related to their privacy, cyber-bullying, and cyber-stalking [5]. Students have to be educated about the presence of online risks, prevention methods, and actions to take if they face any hazard. Thus, an effective cybersecurity awareness program is needed for the students.

An effective program is one developed in an environment crowded with cultural understanding. Margaret Mead defines education as "the culture process, the way in which each newborn human infant, born with a potentiality for learning greater than that of any mammal, is transformed into a full member of a specific human society, sharing with other members a specific human culture [6]. "If that is true, every experience humans obtain by living within a culture is a form of education." Education becomes not a process of conveying knowledge but of co-constructing knowledge in socio-cultural contexts. Interactivity and culture become education and instruction, and the co-construction of reality [1]."

One method for gaining a better understanding of a culture is to make a list of observed differences. There are several cultural differences between Iran and other Western countries, such as e-mail usage, Internet censorship and VPNs, and Islamic culture. Understanding these differences and addressing them during the course design lead to developing a culturally enriched and sensitive program.

1.1 Motivation

This study, with its friendly and interactive course, intend to increase knowledge, skills, and motivation, where the students follow the guidelines completely. The following are the reasons for conducting the research work on the proposed topic.

- Currently, the cybersecurity awareness training is not included in the study curriculum in Iranian high schools [7][8][9]. Hence most teenagers have no training or awareness on how to increase their safety when going online.
- Teenagers from 16 to 18, engage in a great range of online communication activities, such as making friends, giving out personal information etc, and thus they may encounter immense range of communication risks [10].
- It is difficult for teens to gain the motivation in order to follow the guidelines completely. This could be because of the complications and requirement of a certain level of knowledge and skills to follow the guidelines [11].
- In Iran, the most used social media platforms are Telegram messenger and WhatsApp messenger with more than 47 million users, followed by Instagram with around 44 million users, without emphasis on data protection and privacy, cyber ethics, and phishing [12].
- The majority of Iranian people use their smartphones to connect to the Internet rather than personal computers and laptops. More than 50 million Iranian use their mobile phones whereas around 25 million of them use personal computers and laptops [13].
- Already existing cybersecurity awareness program may not be effective enough due to the cultural differences between Iran and West.
- Due to a high level of application filtering in Iran such as Telegram, YouTube, Facebook, and Twitter, almost all of the smartphone users use VPNs so that they can access the mentioned applications [14].

1.2 Research Approach and Methodology

The objective of this research, is to analyze the current awareness level of the students, develop and execute a culturally effective cybersecurity awareness course for high school students of Hormozgan state. Overall research approach consists of qualitative and quantitative research methods. For course design specifically, an instructional design method named ADDIE is used. This model contains five stages of Analyse, Design, Develop, Implement and Evaluate [15]. In addition to the traditional linear ADDIE model, the selected methodology has a third dimension of culture [1]. This model was introduced in 2002 by Thomas and Joseph [1].

During Analyse phase, information on the current state of the student's knowledge on cybersecurity is gathered using a questionnaire. Then, a blueprint of how the course is carried out is drawn in Design stage. Subsequently, the course is prepared according to the design elements specified in the last phase. After that, during the Implement stage, the prepared materials and training are tested utilizing the information gathered in the last two phases. And finally, the proposed program is evaluated and a final conclusion is depicted. The methodology has been described in detail in Chapter 3.

1.3 Research Questions

As mentioned above, the objective of this thesis are analyzing the current security awareness level of the students in Iran, Hormozgan, developing and executing the proposed program. Towards the end, the effectiveness of the cybersecurity awareness program proposed is investigated. Table 1 demonstrates seven main research questions which are subsequently explained throughout this thesis. The questions are answered using background research, a questionnaire targeting 16-18 years old high school students, an interview with one of the school principals, as well as an evaluation method to assess the effectiveness.

Table 1. *Research Questions*

Research Question	**Purpose of the Question**	**Research Method**
What is the current state of the students' cybersecurity awareness level on different concepts of cybersecurity?	To propose a comprehensive course, it is crucial to know the contemporary students' cybersecurity awareness level so that the topics and subtopics are filtered.	Questionnaire and b ackground research
Are there any existing cybersecurity awareness programs focusing on teenagers in Iran?	To understand the pros and cons of the present courses, as well as focus on the needs of the course in case there is no existing program.	Background research
Can already existing Western courses be used?	To substantiate the novelty of the research, the cultural aspects of cybersecurity programs must be evaluated.	Questionnaire and background research

Continues...

Table 1 – *Continues...*

Research Question	**Purpose of the Question**	**Research Method**
Is the ADDIE method with cultural embrace appropriate when designing the cyber awareness program for Iranian cultural space [1]?	To design an effective program, one challenges is the possibility of integrating culture in every step of research.	Evaluation method
What are the cultural differences between Iran and the Western world?	To propose a thorough learning program, the cultures must be well researched so that it would be acceptable by the society with the focus of current concerns of teenagers.	Background research
What is the content and delivery method of the newly designed course for high school students in Hormozgan?	The program's material must be carefully chosen so that it does not clash with cultural values while still addressing the cybersecurity topics about which the students are not trained.	Questionnaire and interview
How effective is the developed cybersecurity program?	To evaluate the success of the research, the effectiveness of the proposed program must be assessed.	Evaluation method

1.4 Contribution

The contribution of this research can be divided into six main sections. Firstly, the lack of study on the current level of high school students' cybersecurity knowledge in Iran, Hormozgan advocates for research to understand their awareness level, and therefore suggest the most suitable course for the students. Once the statistical analysis of awareness on different concepts of cybersecurity has been performed, the survey findings and analysis could be used as literature in any upcoming researches for other states of Iran.

The second contribution is proposing a cybersecurity awareness program in oppose to the lack of awareness courses in the country. As previously mentioned, the absence of a cybersecurity program aimed at the study's focus group is a major issue. Students should be prepared when stepping into the virtual world. They ought to be aware of the vulnerabilities, risks, and dangers of the web. Hence, this study aims to equipt teenagers with the tools they need to increase their safety in the digital world.

The third contribution is the development of a course that is specifically designed to target the cultural sensitivity of the Iran, Hormozgan. Consideration of cultural aspects is crucial, and thus it cannot be assumed that courses developed for Western high school students are effective for Iranian students [1]. Giving an example of Estonia, teenagers posting their photos without any covers on social media is not only acceptable, but it is even encouraged by the families. While, Iran being an Islamic nation, one of the main distresses of the people is the disperse of Hijab-less photos of the females in their respective houses. Therefore the phone security takes another turn as the culture must be taken into consideration.

Another contribution is to share the developed course with public in Iran. The content, slides and teaching instructions will be shared on virgool.io [16]. This website is a free and accessible blogging platform for Iranian people.

Next contribution of this study faces towards the educational sector of the corporate world, aiming to provide a base information for the companies organizing cybersecurity training programs. When such organizations plan to expand their market and develop culturally suitable cybersecurity awareness courses in Iran and culturally comparable countries, this research serves as a goldmine. They will recognize the cultural differences between the West and Iran, as well as other culturally similar countries, and design trainings that are appropriate in the target countries.

Last contribution is to test the ADDIE model with cultural embrace methodology [1]. The author was unable to find any published articles describing the usage of this methodology when developing a cyber awareness course. Therefore, the application of three I's (Intention, Interaction, and Introspection) in every step of the ADDIE model is tested.

In summary, the contributions mentioned above show the novelty and significance this work brings to the academic and educational fields. The research also provides practical contribution relevant to companies in the private sector providing cybersecurity training.

2. Background Research

Throughout the years, there has been many researches to measure the security awareness level and to develop trainings with the aim of educating the users, however, not many focused on Iran's population considering the existing cultural uniqueness. Since this study focuses on creating a cultural training program for high school students, the author discusses other research with similar goals. This chapter contains definitions and approaches developed by other researchers focusing on cybersecurity in general, cybersecurity awareness around the world in comparison with Iran, phone security, effectiveness of a cybersecurity training and Bloom's taxonomy, as a proven educational learning objective. Within this chapter, the following research questions are answered:

- Are there any existing cybersecurity awareness programs focusing on teenagers in Iran?
- Can the existing Western courses be used?
- What are the cultural differences between Iran and the Western world?

2.1 Cybersecurity Definition

The concept of cybersecurity emerged in the world in 1971 [17]. Bob Thomas discovered the possibility of a computer program propelling itself across a network and leaving behind a shadow of its path [17]. He named the program "Creeper," the world's first computer worm with self-replication ability [17]. That was the beginning of cyber threats as known today [18][17]. Over the decades, several academic researchers and media have had different views towards the definition of cybersecurity. Recent cyber-attacks on business organizations and governments have invoked everyone to think more seriously about security issues regarding cyberspace interactions.

The US National Initiative for Cyber Security Careers and Studies in its 2020 Glossary of Common Cybersecurity Terminology, conceptualized cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation[19]." Meanwhile, Rossouw Von Solmas defined cybersecurity as a collection of tools, guidelines, and best practices to ensure the safety and security of the cyber environment and user's assets such as devices, applications, services, and totality of transmitted and/or stored information [20]. In general, cybersecurity involves the protection of online users and ensures the confidentiality, integrity, and availability of systems and data assets.

2.2 Cybersecurity Awareness Definition

NIST demonstrates that "the purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly [21]." Consecutively, IT security awareness and training program are defined as a program that "explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed [21]."

Many studies have been performed on the level of cybersecurity awareness of different target groups globally. For instance, results of a study of three age groups of 8-12 years, 13-17 years, and 18-21 years on Internet usage and cybersecurity awareness were reported in a study conducted in New Zealand in 2016 [22]. The survey results showed that cybersecurity awareness among the surveyed students was generally low, with the lowest level in the 8-12-year age group [22]. Basic terms like "firewall" and "antivirus" were included in the question, as well as more sophisticated terms like "phishing" and "security alert while browsing [22]." The most familiar term for all age groups was "antivirus." They presented the percentage of overall cybersecurity awareness for each age group as: 41% of the participants aged between 18 to 21 were aware of cybersecurity terms, threats, and implementations; solely 32% of the second group (age 13-17) had basic cybersecurity terminology knowledge; and the cybersecurity awareness in students from the age group 08-12 was only 19% [22].

2.3 Cybersecurity Awareness in Iran

Based on a Statista report on Internet usage in Iran, 67.6 million people, or 81.5% of Iranian people's total population, are using the Internet [23]. Shoja Heydari identifies the following as the main threats facing teenagers through the online environment [24].

1. Misuse of accounts: such as gaining passwords and accessing accounts
2. Defamation and harassment: online harassment, which may lead to more serious behavior.
3. Scams: a traditional crime occurring through computer systems, networks, and the

Internet.

4. Disclosure of pornographic images and obscene scenes: one of the psycho-social harms of the Internet is the display of obscene images, which has no result other than increasing depression and stress in teens.
5. Disclosure of images of tragic events: watching violent images poses a great threat to adolescents' mental health and causes encouragement towards violent behaviors.
6. Malware: viruses on the Internet, created by criminals, can disable millions of computers and cause great financial losses.
7. Internet addiction: charms of the Internet make teens spend hours in front of a computer and stay away from other social activities. The most common Internet addiction symptoms can be severe academic failure, decreased social activity, and increased nervous tension and aggression.
8. Creating unhealthy relationships: teenagers widely use chat rooms. These rooms can be excellent places to meet and converse with other students and teachers. Scammers, however, take advantage of several of these spaces. They use other people's information to trap and harass teens by interacting with and meeting them. Relationships between adolescent girls and boys can become more frequent as a result of chat rooms, potentially leading to sexual deviation and other serious issues.

In addition, the researcher mentions some of the consequences of the online threats to be [24]:

- Elimination of the ugliness of pornographic relationships among teenagers
- Emergence of violent behavior as a result of watching violent movies
- Promotions of Western culture and elements of false culture in society
- Change of the values and norms of the society
- Substitution of spirituality and morality by materialistic and worldly thoughts
- Rapid promotion of false rumors and news
- Increase of anti-religious propaganda
- Isolation and staying away from real community environments

A research performed in 2019 by Samouti, Fathy, and Azizipour examined different cyber awareness training methods and validated them within a six-month course for university students, and staff in Iran [25]. According to them, till date, there is no research performed on a well-structured cybersecurity awareness program [25]. Therefore, this limitation calls for an immediate need for a course to be developed. They analyzed eight different methods of information distribution [25]:

- Posters

- Creative animation movies
- Info-graphics
- Web-based games
- Small meaningful sentences posted around the campus
- 30 minutes workshops through seminars or webinars
- 15 minutes educational video clips

Their findings illustrated that interactive methods, such as the game and the animation movie, were more likable by the target groups [25]. On the other hand, people showed less interest in posters info-graphics [25]. They also charted down a 35% reduction in thumb drive exchange amongst students and their willingness to use more secure methods such as emails [25]. Moreover, they discovered a 95% increase in the use of more secure passwords, and only 5% of the target group still uses the old common passwords [25]. Lastly, the access to a suspicious website had a reduction of 40% [25].

It is crucial to mention that there is not much cybersecurity training in Iran for school students. The high school consists of 3 classes and three majors, including Maths and Physics, Literature, and Experimental Sciences [7][8][9]. Unfortunately, there is only one computer course with the title of "Basics of Computer and Informatics" during these three years of studies. This course is only taught in the third year of high school and only to those who have selected Math and Physics as their high school major. This information illustrates that the students' knowledge of computers is relatively low. It also states that schools do not prepare the students to shield themselves against the dangers of the virtual world.

According to a news published on National Institution of Virtual Environment in Iran in November 2020, even though all the classes are organized in distance mode, there is a lack of cybersecurity information provided to school staff and students [26]. Currently, schools have a cyber awareness issue that no one seems to worry about [26]. Schools should be informed on the pros and cons of the software used for teaching, and they should think about the consequences before using any platforms for education [26]. To elaborate more on the topic, the lack of school staff awareness of cybersecurity is worrisome. This is unfortunate that not many initiatives have been taken to improve the school staff's cybersecurity awareness level [26]. Therefore, it is clear that no initiative has arisen intending to increase the students' cybersecurity awareness.

In Iran, advertising the importance of cybersecurity is a relatively new initiative. There are only few online courses over the Internet in Persian language, which mostly feature employees' awareness. Amongst them, the online course taught by Nozari is a comprehensive program discussing the topics such as Intranets, firewalls, and different jobs in the cybersecurity field [27]. His teaching method involves use of video recordings explaining the concepts and distributing information [27]. Another online course is "Teaching Cyber Security", taught by Heydari, which covers cybersecurity concepts such as cybersecurity attacks, standards, tools, risk management, and digital signature through 15 sessions [28]. The course is taught within different pages containing related information for the topics covered [28]. Another program is the course brought by Evand.com [29]. This course is a 2 hours program focusing on cybersecurity practices for businesses and companies only, and therefore, the focus group is not pupils [29]. Another workshop on cybersecurity was held by the Iranian Police, with the title of "Trusting unknown individuals in the virtual environment is dangerous [30]." In this workshop, the target audience was female high school students in Bojnoord, Razavi Khorasan State of Iran [30]. Despite the fact that it is a workshop to disseminate material, there is no evaluation of its effectiveness.

Hormozgan Province

Hormozgan is a state located in the south of Iran. In general, the people of Hormozgan speak different dialects, which are utterly different from Persian; however, children learn Persian from an early age because it is the medium of communication in schools [31]. Shaykh Baygloo reveals that Hormozgan is one of the most deprived states of Iran [32]. In her study, she used infrastructure, education, economics, health, and agriculture indicators to analyze Iran's states and rank them [32]. Unfortunately, at present, there is no study found on any research performed on the state of Hormozgan's student's knowledge and awareness on any topic, needless to say, cybersecurity. Searching through English and Persian literature reached a dead end in data collection concerning the matter.

2.4 Phone Security

The number of smartphone users is increasing daily regardless of age groups, nationality, and educational background. The more mobile phone devices are used, the more information they hold, and therefore, they are more prone to cyber-attacks [33]. However, while users' awareness in the domain of personal computers is relatively high, previous studies have shown that the security awareness level is significantly lower for the mobile platform [33].

Bitton and colleagues proposed a taxonomy of mobile users' security awareness with the help of Kruger and Kearney's previous study, that developed a prototype for assessing information security awareness [33][34]. Bitton and his partners proposed a hierarchical structure of technological elements associated with mobile security awareness alongside a hierarchical structure of the psychological dimensions and components [33]. Both structures are illustrated in Figure 1 and Figure 2 respectively. They enrich technological security aspects with users' psychological traits by considering each aspect in light of three psychological dimensions: attitude, knowledge, and behavior [33]. "For instance, a user with a high level of mobile security awareness is a person who perceives that malware infection is a common threat among users; a person who perceives malware infection as a risk to his/her phone or privacy; and/or a person who perceives that using an updated antivirus is an effective action to defend his/her smartphone [33]." The analysis demonstrated that knowledge, attitude, and behavior are required for smartphone user to increase their awareness and mitigate cyberattacks [33].

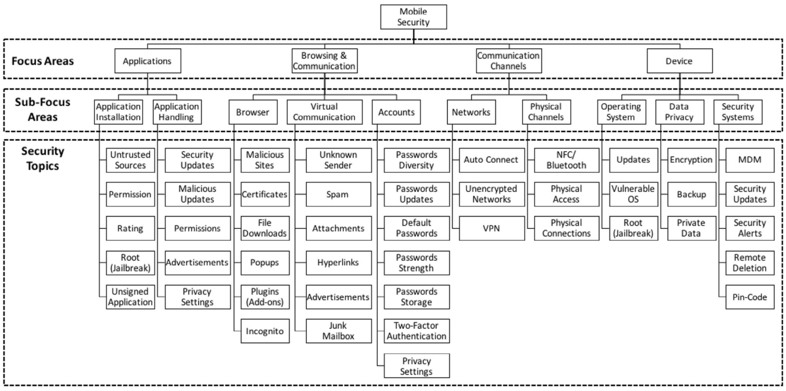


Figure 1. *The hierarchical structure of technological elements associated with mobile security awareness. [33].*

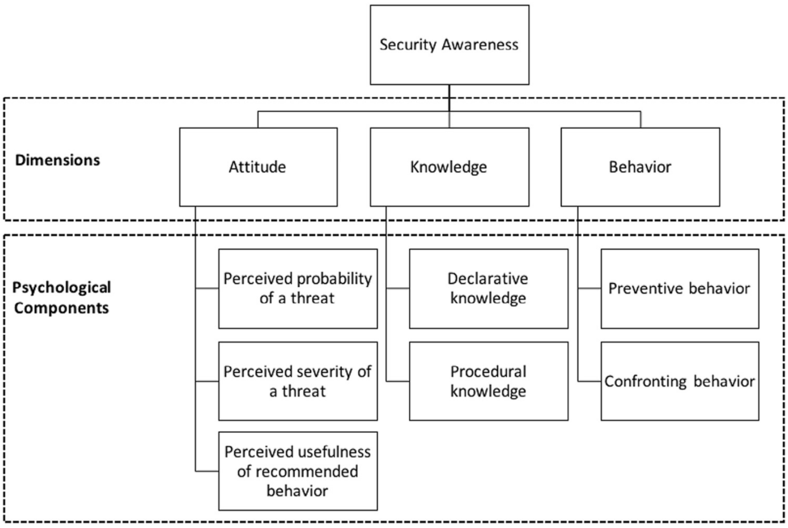


Figure 2. *A hierarchical structure of the psychological dimensions and components. [33].*

In another study performed by Al-Hadadi and Al Shidhani, they address the challenges and problems in dealing with smartphone security threats [35]. They imply that, in general, people's awareness of phone security concepts is deficient and in need of immediate action [35]. The results gathered from their research are listed below.

- Trust Factor: 5% of respondents said they don't trust smartphones to send and receive critical and confidential information over the Internet. In contrast, 24% of respondents had reservations about trusting smartphones, while 31% are confident in exchanging sensitive information through smartphones and the Internet.
- User Familiarity: more than 50% of the users did not have any information on issues related to smartphone security and security best practices.
- User Confidence: The most popular reason for installing an application is that a family member or acquaintance has already installed it.
- Incident Reporting: 48% of respondents had no idea where to report if an incident occurred, and 25% had never heard of the agencies in charge of managing such accidents.

Unlike Al-Hadadi, who claimed only 45% of people use phone devices to store personal data, Androulidakis argues that 62.72% of users save such information on their mobile devices [35][36].

Research conducted by Koyuncu and Pusatli in Ankara, Turkey, to measure the awareness level of a wide range of participants of different ages, education levels, and professions reached similar results as the aforementioned examinations [37]. They summarized their findings as follow:

- An overall awareness level is low and needs improvement.
- Youngsters aged less than 21 and adults aged more than 50 have the least cybersecurity awareness level.
- Higher education influences having a better awareness level
- The group having IT security training has the highest awareness level
- Low-security awareness levels among phone users

Moreover, Parker, Ophoff, and Van Belle added information on the awareness and adoption of security controls by smartphone users [38]. They confirmed that the adoption of security controls is associated with language and gender factors [38]. They suggest additional training for non-native English speakers to grasp cybersecurity concepts [38]. They also state that the female users have less awareness and inclination to adopt controls which are often technical [38]. "Conveying the purpose and functionality of such controls in a nontechnical way is crucial as more users from developing countries become smartphone owners [38]."

On the existing mobile phone security trainings across the web, two of them are analyzed in this study. The first one is available on Coursera and taught by (ISC)² Education Training

[39]. Throughout the course, there is material on data and account security, passwords, networking and mobile security, malware, and social engineering [39]. Although the content is comprehensive and is developed to target beginners, they are very generic, and there is no focus on culture. The second training is published on the Social Media Training website, and Eric Schwartzman teaches it [40]. In this training, mobile social networking, Facebook, Twitter, and Google multi-factor authentication, mobile app security and location-based social networking threats, public wireless Internet access via laptop, iPhone, or Android, and safely disposing of handheld and other mobile data storage devices are all topics covered [40]. This training also contains a high level of beneficial information; however, similar to the former training, it is general, without a specific focus group.

2.5 Cybersecurity Awareness Programs Around the World

In a cybersecurity awareness program by Das, and partners, they proposed a course called "Cybersecurity for Future Presidents [41]." The course had three learning objectives that aligned with the educational goals for non-computer science students [41]. The goals were students achieving technical foundations, policy foundations, and critical thinking [41]. Each objective has several class topics mapped to it, for example, data representation supports technical foundations, and cyber warfare supports policy foundations [41]. To provide students with the opportunity to increase their critical thinking skills, some in-class debates were introduced [41]. Based on the results gained, the student's awareness of cybersecurity issues had increased [41].

Another content-based cybersecurity awareness program is "You Are the Key to Security" which McCoy and Fowler introduced [42]. They discovered that when adapting a program, it must be flexible in order to satisfy current and future demands while remaining relevant to the target audience [42]. This cybersecurity awareness initiative seeks to improve people's attitudes and behaviors toward information security through creating metrics to assess audiences' cybersecurity knowledge as well as the program's success rate, and eventually discussing critical information security concerns on campus [42]. The program focused on two target groups of students and faculty staff. The training content list consisted of password safety and security, Internet and email security, and Family Educational Rights and Privacy Act (FERPA) [42]. The delivery methods used were targeted mass emails, articles in the monthly technology newsletter, and ads in the student newspaper [42]. The program proposes a monthly topic and additional activities to ensure reaching the educational objectives. For instance, the monthly topic in January was "Password Safety and Security [42]."

Cai and Arney present a top-down and case-driven (TDCD) cybersecurity teaching model

[43]. They argue that this model fills the gap between university education and industry need [43]. Their case study covers target breach, DDoS attack, and anthem breach [43]. The course topics include email phishing using social engineering, web security, network security, firewalls, cryptography, etcetera, having ten hands-on labs, which help students practice classroom learning in a simulated virtual environment [43]. Finally, there is a final exam to assess the students' knowledge of cybersecurity [43]. The course was tested for three consecutive years, and the results of these skills and knowledge of the students showed improvements within three years [43].

Lastly, Smith and Ali introduced a cybersecurity awareness program in 2019 with the following steps [44]:
Step 1 – The Setup. Students are told that they will be doing game programming and to copy a workspace containing all the source code for the games to the desktop. They are also asked to create a word document to list their secret players' names and save these files on the desktop.
Step 2 – The Distraction. While a presentation on object-oriented game programming is given, they are distracted from the fact that they have just created files on their computer containing sensitive information.
Step 3 – The Draw. After that, the students are guided to open the workspace and make few changes to prepare for the helicopter attack game.
Step 4 – The Hack. Unknown to the students, the helicopter game has a separate hidden thread of execution, with access to the desktop directory only, which finds the two documents they created on the desktop at the start of the lab and sends them to the remote computer which the instructor logs into.
Step 5 – The Announcement. At this point, the instructor announces, "You've been Hacked," and shows them the file directory on the remote computer. To emphasize that the files have actually been stolen, few of the files are opened on the computer with students' consent.
Step 6 – The discussion. While the program restricted itself to finding and sending the documents on the student's desktop, it could have found files of any type anywhere on the computer. While files were sent to a remote computer, they could have been sent to any place in the world. While the program was only used to steal information, it could have installed a virus.
Step 7– The prevention. Few prevention techniques such as confirming the source is trustworthy, use of anti-malware products, installation of firewalls, account management and limiting capabilities are discussed.

Moreover, the lecture/lab has been presented to various audiences, including middle school students, high school students, school teachers in a cybersecurity summer camp, and the college students in a lab session to introduce a computer science course [44]. The results showed that amongst the target groups, newcomers and teachers were most responsive towards being hacked [44]. In contrast, the least responsive group were middle school students [44]. They understood that the files have been stolen; however, they did not know that this information can have life-impacting consequences [44]. They claimed the technique was effective in the context of Protection Motivation Theory (PMT) [44].

2.6 Design and Effectiveness of Cybersecurity Awareness Programs

This section discusses number of key points used to identify the effectiveness of a cybersecurity training discussed by several researchers. One of the main aspects of a successful program is the design method chosen. Design choices directly reflect on the effectiveness of a program. Here, the author introduces Bloom's taxonomy which is known as one of the evident and efficient instructional design methods in the education world. With the help of this taxonomy, a course is designed and developed in Chapters 5 and 6.

Holdsworth and Apeh claim that their background research identified the following elements to identify successful security awareness campaigns [45][46][47][48].

- Achieving management support
- Be creative – provide a fresh and fun learning process
- Relevant Content – each department will only learn content relevant to them
- Emotional involvement – explain the impact to them and the company
- Use multiple forms of media – videos, posters, stickers, and pictures
- Incentives – reward the best learners
- Regularly reinforcing what has been learned
- Metrics – establish a way of measuring the effectiveness and impact of the course

While Bada, Sasse, and Nurse's research on the reason behind cybersecurity campaigns' failure revealed that two main elements influence online behavior changes [49]. The first element is personal factors in which personal motivation and personal ability are introduced as its most potent sources of influence [49]. The second element is cultural and environmental elements [49]. For example, In collectivist cultures, individuals tend to define themselves in terms of their relationships with other members, and therefore, they tend to avoid behaviors that cause social disruptions [50][49]. Hence, they favor the strategy of prevention over promotion. They tend to avoid adverse outcomes rather than approach positive outcomes [51][49]. Thus, cultural contexts need to be addressed when creating cybersecurity awareness campaigns [49].

In the research mentioned above, a section presents the pitfalls that must be avoided to have a successful cybersecurity awareness program [49]. The first refers to incorrect defining of security awareness [49]. Secondly, understanding of compliance awareness, which is not necessarily equate to creating the desired behaviors [49]. Third, lack of engaging and appropriate materials [49]. Fourth, lack of illustration that awareness is a unique discipline, and fifth, lack of assessment of the awareness programs [52][49]. Sixth, rather than planning several training activities, concentrating on a single subject or danger which does not provide the thorough training needed [53][49].

Siponen states that there are two categories outlined in cybersecurity awareness programs, framework and content. The framework can be approached by quantitative research, while content is more of an informal interdisciplinary field, and it should be approached using qualitative research methods [54].

Bloom's Taxonomy

In order to design effective learning experiences, the course development should follow and/or build upon the existing learning theories and approaches. Throughout the years, there have been many learning taxonomies introduced by different researchers. Namely, Six facets of understanding, SOLO Taxonomy, Fink's Taxonomy, and Bloom's Taxonomy [55][56][57][3][58]. Here, Bloom's Taxonomy is analyzed to have a clear understanding of the order of skills gained through learning. This taxonomy was first developed in 1956 by Benjamin Bloom with the help of some other collaborators and then revised by a group of cognitive psychologists, curriculum theorists, instructional researchers, and testing and assessment specialists in 2001, [59]. This taxonomy consists of 6 levels. Starting from the bottom, they are named Remembering, Understanding, Applying, Analysing, Evaluating, and Creating [3]. Figure 3 demonstrates the taxonomy stages and the relation between them. The following is a simple definition of what each level stands for [60]:

Remembering: To recall the information learned, such as memorizing and defining the terms and facts
Understanding: To know and understand a concept so it can be explained to someone else
Applying: To apply the concepts learned to solve a problem
Analysing: The ability to breakdown the knowledge into parts and effectively analyze a situation to apply the concepts learned to solve a problem
Evaluating: The ability to judge, criticize and have recommendations for an idea
Creating: The ability to concatenate ideas to form a new solution.

According to Armstrong and the authors of the revised version, there are several benefits

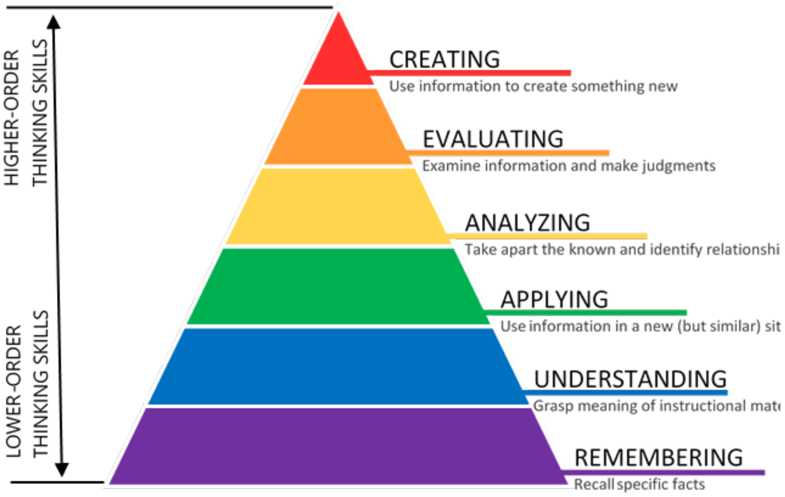

HIGHER-ORDER THINKING SKILLS
LOWER-ORDER THINKING SKILLS
CREATING
Use information to create something new
EVALUATING
Examine information and make judgments
ANALYZING
Take apart the known and identify relationshi
APPLYING
Use information in a new (but similar) sit
UNDERSTANDING
Grasp meaning of instructional mat
REMEMBERING
Recall specific facts

Figure 3. *Bloom's Taxonomy's 6 Levels of Learning. [3].*

in using Bloom's taxonomy [61][59]. In Armstrong's research report, they are listed as follow [59]:

1. "Objectives (learning goals) are important to establish in a pedagogical interchange so that teachers and students alike understand the purpose of that interchange."
2. "Teachers can benefit from using frameworks to organize objectives because organizing objectives helps to clarify objectives for themselves and students."
3. "Having an organized set of objectives helps teachers to:"
   - "plan and deliver appropriate instruction;"
   - "design valid assessment tasks and strategies; and"
   - "ensure that instruction and assessment are aligned with the objectives."

2.7 Influence of Culture on Cybersecurity Practices and Values

In previous eras, the criteria for determining which countries are superior to others included outstanding literature, capital, and military capabilities. However, nowadays, these standards changed to communications and the countries' ability to discuss, share, and provide media transparency. One of the main features of the current era is that, there is no need to use the old ways to transmit our thoughts, believes, and knowledge. With the least possible time and funds, and the most geographical coverage, faith, opinion, and ideas can be manifested. However, the usage and access to the information vary amongst different countries. For example, there is a substantial difference between Internet access amongst coin tries in the EU alone. Nordic countries such as Estonia, Finland, and Norway have complete access to the Internet [62]. In contrast, this value reduces a lot when it travels to southeast European countries such as Slovakia, Romania, and Hungary [62]. Giving an example of Muslim countries, access to information, transparency, and clarity also reduces in countries like Iran and Malaysia. For instance, the website contains seditious, and harassment for the Muslim people and pornography websites are filtered in the two countries while the same contents are not filtered in Estonia [63]. In short, culture and religion play a vital role in defining how much the Internet content is reachable for the citizens of the country and how the different tools published on the Internet are being used by the nations.

Fast and cheap access to the Internet causes the rapid publication of events, hence advancing knowledge in any society. With these new technologies, communities, way of living, cultures, values, and even family relations are affected. However, depending on the belief strength and the freedom given to people of any culture, these changes may take effect or be discarded by the community. For Iran's case, changes such as publishing content against Iranian scholars' values, policymakers, and sensual topics are prohibited [64]. Karim Zadeh discusses that the changes brought to Iran's culture through technological advancement are undeniable [65]. However, authorities must control these new changes, and only those in harmony with the ruling government's goals must be allowed [65]. He suggests that Iranian authorities could take three approaches to manage the amendments [65]. The first way is not to take any actions towards the changes, which is highly ill-advised as the cultural and religious roots are significantly damaged [65]. The second way is to prevent any technology and its related changes from entering the country, which is ultimately impossible due to VPNs' usage to overcome filtering [65]. The third and the best-proposed way is to change people's mindsets to align with the government's cultural and religious principles [65]. This research shows that religion and culture are an essential part of the Iranian community. If any information, such as cybersecurity awareness training, is not in line with those principles, society would not accept it. Therefore, the content delivered must be tangible and understandable by the Iranian audience.

Before listing down the cultural differences, there is a need to know what really culture means. Helen Spencer-Oatey defines culture as "a fuzzy set of basic assumptions and values, orientations to life, beliefs, policies, procedures and behavioral conventions that are shared by a group of people, and that influence (but do not determine) each member's behavior and his/her interpretations of the 'meaning' of other people's behavior" [66] [67]. Therefore, every new belief or behavior that enters society is measured against a predefined set of values to evaluate whether they are aligned with the community's accepted culture.

"Weber emphasized three arguments regarding religion and society: (1) how a religion relates to a society is contingent (it varies); (2) the relationship between religion and society can only be examined in its cultural and historical context; and (3) the relationship between society and religion is slowly eroding" [68][69]. Additionally, in the social sciences, there are many meanings of the word "culture," each focusing on a particular phenomenon: mind, behavior, symbols, or artefacts [70]. "According to sociologists and anthropologists, culture embraces all that constitute "ways of life" [70]." Since it is difficult to define what does not constitute a way of life in society, an all-inclusive definition of culture as "ways of life" appears to be broad. What matters is the diversity of cultural phenomena, such as ethnicity and religion, as well as secular principles and tradition, and the political implications of these phenomena [70]. These theories focus upon the political impact of ethnicity, religion, values and tradition [70]. Within this research, the term "culture" is used to interpret the different cultures of Iran concerning religion, politics, and legal restrictions such as state censoring.

Cybersecurity training and awareness programs promote the change of user behaviors and attitudes. However, cultural aspects of the people following the introduced guideline need to be considered to ensure quick information distribution, understanding and application. Similarly, Garett suggests that culture is a set of traditions molded by religion, ethnicity, language, and history [71]. Culture serves as a lens through which a society views the world. Therefore, the governments and organizations should provide awareness approaches that include training lined up with culturally sensitive cybersecurity policies and Education. Another uniform research completed by Al Shehri implies that cultural values influence knowledge and behavior towards cybersecurity [72]. The main objective of this research was to identify whether cultural differences would affect students' understanding of information security. The author's approach to conducting this research was to analyze the level of awareness, knowledge, and behaviors of the students enrolled in two universities in South Africa through a vocabulary test. The results revealed that a person's place of origin and mother language significantly impact their awareness levels. In short, the cultural factor is a very vital element that must be considered when designing cybersecurity awareness training.

With those being said, few items need to be considered when designing cybersecurity training for Iranian citizens. These cultural aspects are well blended into the Iranian culture, and therefore, if missed, the course effectiveness would reduce.

2.7.1 Islamic Hijab Culture

As the use of cyberspace grows on a daily basis, Iranian policymakers' concerns about the state of religion increase [73]. This is due to a strong Islamic belief leading Iranian people and organizations' thoughts and mindsets [74]. They have been several researches done on the negative side effects of cyberspace on religion. Bakhtiyari and Azizkhani argue that cyberspace weakens the religious identity while strengthens the modern and global identity

[73][74]. They claim that presence in social media memberships causes a person to gain and strengthen this global identity while sacrificing one's religious identity [73][74].

Hijab has various meanings in the dictionary, but the most common meaning is a thing that veils, conceals, hides, covers, or protects because it prevents seeing or beholding [75]. In the Islamic world, this term is defined as a Muslim women's dress code covering her hair and body, and it is one of the most important rules to follow from an Islamic perspective [75]. Furthermore, due to many Iranian families' Islamic values, posting Hijab-less images on social media, whether deliberately or accidentally, is frowned upon; and, if the Hijab-less photo is leaked without the owner's permission, it is a crime [2]. Some researchers oppose this statement, including Karimi, who contends that regardless of government rules forcing Iranian women to wear Hijab outdoors, they use cyberspace to publish their Hijab-less images to represent a new version of Iranian women who redefine their identity through a combination of modern and traditional attitude [76]. They no longer identify themselves with being a traditional Islamic woman [76]. Even though the above statements are factual, it is essential to emphasize that due to Iran being a big country with over 82 million people, big cities' lifestyles are different from those of borderline states [77]. The focus group of this research is High school students of Hormozgan state in Iran. This state has been noticed as one of the deprived states in Iran, and therefore, the culture and beliefs are still intact and not much affected by the information absorbed from the Western media [78].

In consideration of the preceding, the Hijab plays a vital role in the lives of most of the non-capital residents of Iran. Unfortunately, it is common for incidents such as leakage of the Hijab-less photos happening in these areas, and as a result, households are shattered. As an example, the phone of a 19-year-old girl who was recently married got hacked by one of her husband's relatives, and hence, she was threatened and blackmailed. This incident ended with her writing a police complaint and her getting a divorce at an early age [79]. Due to a lack of awareness about cybersecurity, regretfully, such incidents effetely happen in Iran. Therefore, this deems the necessary attentiveness to Islamic Hijab principles when adopting technology and its related information and designing a new cybersecurity awareness course and training for Iranian students.

2.7.2 Censorship and VPN

One of the major goals behind Internet development was to increase the communication and connection between people worldwide. Nevertheless, it is censored almost everywhere and strictly filtered in a few countries [80]. Iran is one of them [81]. Censorship is defined as the institution, system, or practice of reading communication and deleting material considered sensitive or harmful [82]. Currently, Iran is ranked 22 among the most ranked Internet usage countries by any device, including mobile phones [83]. There are six Internet Service Providers (ISP) in Iran, with the biggest one named "Communications in Iran," owned by Iranian government [84]. All these providers must comply with the rules set by the policymakers. They intentionally limited the bandwidth as a means of precautionary measures [85]. According to a report published in 2019 in the Iran International News website, 35% of the most viewed websites and applications worldwide are filtered in Iran, and YouTube, Facebook, Twitter, and Telegram are amongst them [85]. In research conducted by Simurgh Aryan, Homa Aryan, and J. Alex Halderman, the extent of the censorship inside Iran was evaluated. They investigated the most visited websites based on Alexa web traffic rankings limited to 500 in 18 different areas [14]. The results are shown in Figure 4 .

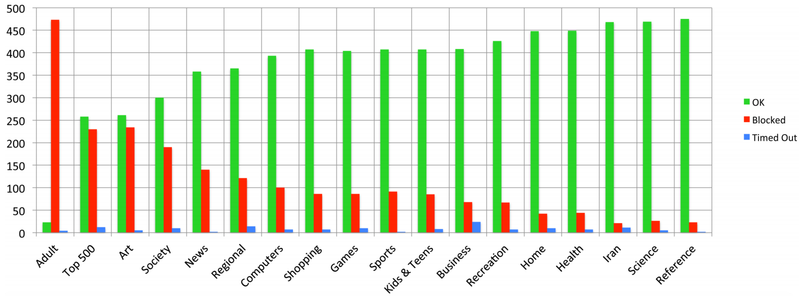


Figure 4. *Effects of Iranian Internet censorship on the top 500 websites for 18 Alexa categories [14].*

Due to the overly performed Internet censorship in Iran, people tend to use VPNs regularly to access the content [14]. The VPN technologies are established to transform the Internet into a secure global network [86]. Although in general, using VPNs is considered a good habit, however, if the VPN is not downloaded from an authorized source, it could lack encryption and lead to traffic leaks, have malware presence, allow the third-party user to track and access sensitive phone permissions, and other drawbacks that jeopardize the security of mobile devices [86]. In Iran, unfortunately, the knowledge of what VPNs are and their functionality is relatively low, and people tend to define VPNs as an app that allows one to connect to Telegram applications [87]. Considering this, VPNs' excessive use without prior knowledge of their safety and reliability could lead to nonreturnable damages.

Iranian constitution restricts a broad range of topics relating to religious and political expression [88][14]. Official institutions ensure certain transparency for their censorship activities by informing users that certain content is blocked [88][14][89]. Triggering censorship includes international news coverage of sensitive topics, political opposition, sexual topics, online activities of ethnic and religious minorities, as well as human, digital, and women's rights groups [88][89][90]. As shown in Figure 4, in the alignment of pornography being censored in Iran, the topics of harassment and even sex education are not allowed to be taught in schools. In high schools majority of courses focus on Maths, Science, and Humanitarian [7] [8] [9]. With that being said, when conducting training on cybersecurity, limitations of discussed topics must be taken into consideration. For example, in a course developed by Martina, Zucule de Barros, and Horst Lazarek, the following topics were identified as essential incorporate countermeasures to be taught in school for safeguarding themselves against online problems [91]. Whereas, in Iran's case, the topics of child pornography and sexual images or messages are certainly prohibited from being discussed with high school students [88][89][90].

- Internet surfing
- Social networking
- Cyberbullying
- Child pornography
- Cyber identify theft
- Online privacy

2.7.3 Tools Usage

According to Tajik Ismaili and Yousef Zadeh's research on the types of Internet usage amongst High school and university students in Iran, they found that searching for scientific topics are the most used reason for the Internet amongst the students [92]. Their findings are shown in Table 2.

Table 2. *Types of Internet Usage Amongst Students in Iran [92]*

Usage	**Never (0)**	**Seldom (1)**	**Sometimes (2)**	**Usually (3)**	**Always (4)**	**Average**
Searching for Scientific Topics	8.2	6.1	37.8	35.7	12.2	2.37
Chats and Communication	17.4	20.5	25.6	21.0	15.4	1.96
Following up News	22.4	18.9	24.0	18.4	16.3	1.87
Downloading Musics and Movies	12.8	27.7	30.3	20.5	8.7	1.84
Social Media Membership	16.5	18.6	38.6	24.7	4.6	1.82

Continues...

Table 2 – *Continues...*

Usage	**Never (0)**	**Seldom (1)**	**Sometimes (2)**	**Usually (3)**	**Always (4)**	**Average**
Search for General Topics Like Weather, Health, etc	15.9	32.3	29.2	16.9	5.6 1.64	
Checking Emails	18.0	27.8	33.5	13.4	7.2	1.63
Trading Good and Services	41.0	32.8 20.5	3.6	2.1	0.92	
Marketing Goods and Services	53.3	23.6	16.9	5.1	1.0	0.76
Uploading Content in Weblogs and Websites	58.0	21.8	14.5	3.1	2.6	0.70

According to Table 2, it can be concluded that among students in Iran, email usage is minimal, and people tend to download media from any sources on the Internet more than checking their emails. Additionally, the minimal usage of email addresses can be seen through the registration forms of Iranian websites. For instance, famous websites in Iran such as Bama (a platform for car marketing) only require phone numbers to sign up [93]. In other cases, such as the iran-tejarat website, upon the registration, the field holder specifies, "Please attention that email does not start with www." [94]. This indicates another cultural aspect when designing the course. When teaching the students about clicking unknown links, there should not be mentions of email; instead, the links to download media could be used as an example.

2.7.4 English Language Limitation

Another crucial point to consider is proficiency in the English language. English is the language of computers. The majority of commands, instructions, errors, warnings, even malware messages such as the ransomware notes are in English [95]. 98% of the content online is in English [96]. Without knowing English, learning and even being updated with the world's news and contents is challenging.

Although English is taught in Iran schools, inappropriate textbook materials and a translation and grammar-based approach to English teaching have resulted in Iranian students' poor English language proficiency [97]. While the schools are not productive in English language teachings, there is a growing interest in English language learning, mostly in big cities such as Tehran, Esfahan, Mashhad, Shiraz Tabriz, and Kerman, even though English is not a second language [98]. However, for Hormozgan, this research's focus group, this is not the case. As previously mentioned, since this state is impoverished, English literacy is expected to be minimal [32]. Therefore, majority of the students' knowledge in English should be limit to the grammar that is taught in school.

Furthermore, Hormozgan state students' lack of English proficiency raises the possibility that they could develop the habit of clicking on any button they see on the screen when a pop-up message appears, without actually understanding what the pop-up is about or what are the consequences of clicking on it are.

2.7.5 Free WiFi

According to a report published on the WiFiMap website, there are 18,283 free WiFi locations in Iran, with 5,000 of the spots located in Tehran [99]. With that being said, the probability of free WiFi being presented in the deprived states such as Hormozgan is close to 0 percent. In recent years, four of the Internet Service Providers (ISP) in Iran took the initiative to provide free published WiFi in the airports and big shopping malls of Tehran, and other big cities [100]. The ISPs are Hamrah-e Aval, Irancell, Raitel, and Asiatk. So far, more than 60 locations around Iran are equipped with public WiFi with a limited bandwidth of 150 to 200 megabytes per user [100].

This information describes another cultural distinction in Iran. Lack of free public WiFi would emphasize the difference between the topics discussed in the West and Iran. Public WiFi connection is a constant in most cybersecurity awareness courses developed in the US and the EU. However, adding this concept to training focusing on Iranian society would be fruitless.

2.7.6 Lack of Browser Cookies

Kaspersky weblog defines Cookies as "text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience" [101]. These days, upon visiting almost every website out there, we see the pop-up encouraging us to agree with the website Cookies storing our information. However, this is not the case in Iran. According to Tahmasebi, in a blog posted on the Karsazsho website, the top most visited Iranian websites are Aparat.com, digikala.com, varzesh3.com, shaparak.ir, namnak.com, telewebion.com, emofid.com, divar.ir, and tsetmc.com [102]. However, when all of the websites listed were accessed, none of them had the Cookies usage agreement pop-up displayed. This brings another point that if the Iranian populations are taught on what cookies are and their advantages and disadvantages, the content would be irrelevant for them as they are not likely to interact with them every day.

3. Methodology

This chapter elaborates the methods used to conduct the research. There has been many studies suggesting different instructional design models throughout the years. Amongst them, Gagne's Nine Events of Instruction, and Merrill's Principles of Instruction can be named [103][104][105]. This thesis applies ADDIE model with cultural embrace elements to achieve the results [1]. ADDIE model's first appearance in the world can be traced back to the 1970s [15]. The US Army approached Florida State University's Center for Educational Technology with a request to develop a better way of training to improve soldiers' knowledge and skills while reducing the time and budget resources [15]. At that time, the model was known as instructional systems development (ISD), and at present, the two terms are synonyms [15]. The ADDIE model known today was developed in 1978 by Dick and Cary and revised by Russell Watson in 1981 [106]. Since then, it was considered essential in developing educational and training programs [106].

In the beginning, the ADDIE model was a two-dimensional model with mono-directional relations, and linear [1][107][108][109]. In 1996, Ritchie and Hoffman introduced a new variant of the ADDIE model, which allows the model to be two-dimensional and bi-directional [1][110]. This design provides an opportunity for the ADDIE model to meet the requirements of an unstable environment [1][110]. Figure 5 and Figure 6 visualize mono-directional and bi-directional ADDIE models respectively. In today's literature, it can be seen that different authors tend to accept the ADDIE term as an umbrella term, moving on with developing divergence models based on the original ADDIE model [111].

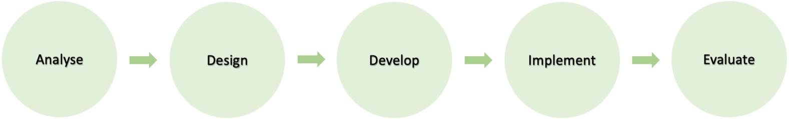


Figure 5. *Mono-directional ADDIE Model Design [1].*

ADDIE research model consists of 5 stages. Bell and Shank provide a general definition for ADDIE as follow [112][113]:

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 [112][113].

This model is a well-known methodology used by professional instructional designers for technology-based teaching and training [114][106]. ADDIE has been identified as a successful interactive design model due to its few characteristics: providing appropriate quality design, clarifying the learning objectives, constructing organized content, proposing interactive student activities, and binding assessment to learning objectives [115][116]. Although the qualities mentioned above do not limit to the ADDIE model only, it operates as a management tool for meeting a standard quality [115][116].

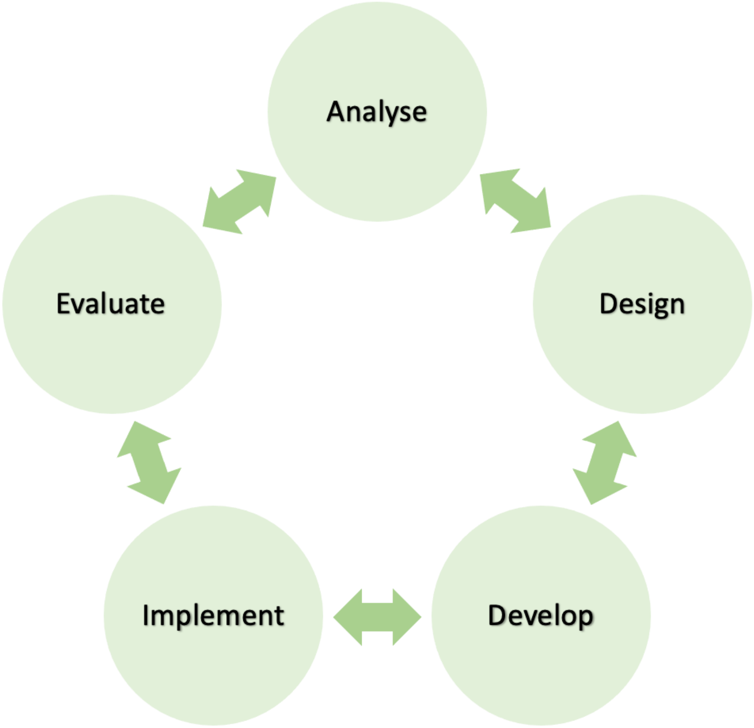


Figure 6. *Bi-directional ADDIE Model Design [1].*

However, there have been several criticisms targeting the ADDIE model throughout the years. One of the limitations is called as "front-end loaded" feature, meaning the model focuses mainly on the interactive design's process, such as content design, while leaving out the interaction between the instructors and the students and suggestions on teaching technologies of assessment methods [117][116].

The program designers must engage with the people with whom the course is designed in order to formulate a culturally appropriate design [1]. Therefore, this researches utilizes a suggested alternate ADDIE design introduced by Thomas, Mitchell, and Joseph, proposing a third dimension to the ADDIE model as culture [1]. The purpose behind this selection is to test the usability of their submitted methodology. They suggest 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 [1]." The mentioned research introduces three I's, as Intention, Interaction, and Introspection, to be implemented in each step of the ADDIE model [1]. This additional dimension allows the culture to blend in with the proposed course thoroughly. The proposed design is illustrated in Figure 7.

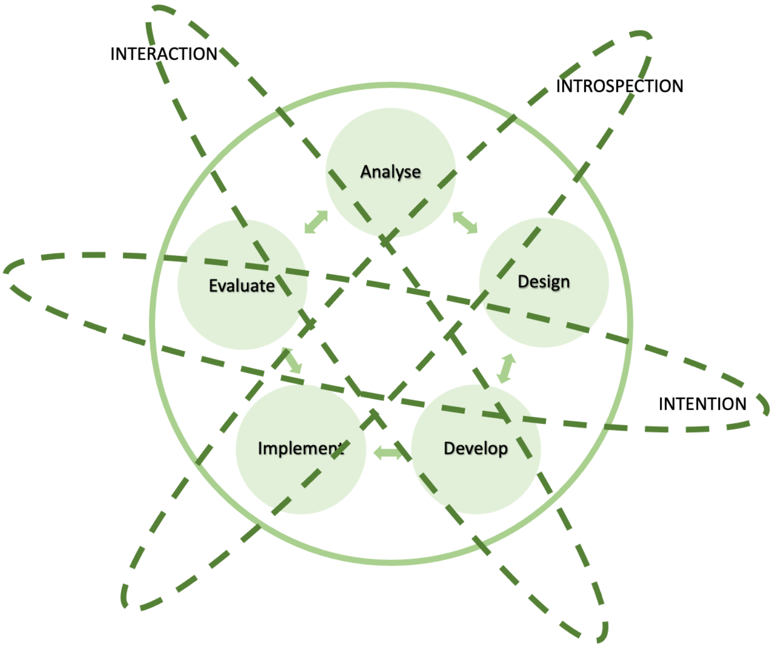


Figure 7. *Three Dimension ADDIE Model Design [1].*

3.1 Analyse

To complete the ADDIE model's Analysis step, eight different analyses are conducted. In particular, the analysis is performed on the program's needs, students' current knowledge, content to be taught, cultural differences, technical specifications, online environment, and desired learning outcomes and research limitations.

An initial questionnaire is sent out in order to obtain information on all of the analyses mentioned above. The responders are high school students of Hormozgan province. Additionally, an interview with one of the school's principal has taken place to gain more information on the cultural aspects and rules and regulations of teaching in Hormozgan. The data collection process is done using convenience sampling.

The thought of listing elements is adopted from Educational Technology website [118]. The concept is implemented below and in the subsequent sections of this chapter. By the end of the Analysis chapter, the following concepts are discussed.

- Importance of developing a cybersecurity awareness course for Hormozgan high school students (Discussed in Chapter 2, Section 2.3)
- Background of the target group such as age, gender, previous experiences with cybersecurity awareness courses, cybersecurity knowledge level, cybersecurity incidents encounter, and cultural backgrounds. (Discussed in Chapter 4, Section 4.1)
- Content of the course (Discussed in Chapter 4, Section 4.2)
- Desired learning outcomes in terms of knowledge and skills (Discussed in Chapter 4, Section 4.5)
- Cultural differences distinguishing Iran from the rest of the world (Discussed in Chapter 2, Section 2.7)
- Current culture of education in Iran (Discussed in Chapter 4, Section 4.3)
- Technical specifications needed for the class (Discussed in Chapter 4, Section 4.4)
- Preferred online learning environment (Discussed in Chapter 4, Section 4.4)

3.2 Design

The next step is to design the awareness program based on the study's information gathered in Analyse phase. This chapter's objective is to draw a clear outline on how to carry out the program. One of the features of the program that should be kept in mind is its quality. "Quality teaching transforms students' perceptions of their world, and the way they go about applying their knowledge to real world problems [119]." In this context, the designed course should be as practical as possible, making sure that the Apply level of Bloom's theory is met and the content and exercises shared motivates the students to utilize their knowledge when surfing the web.

To carry out the Design phase, learning objectives, communication tools, course execution date, course content, helping tools, and course evaluation are designed and outlined. By the end of the Design chapter, the following elements are addressed:

- Number of students per class and process of informing them about the class (Discussed in Chapter 5 Section 5.1)
- Tools used for establishing the class (Discussed in Chapter 5 Section 5.2)
- Instruction language (Discussed in Chapter 5 Section 5.1)
- Number of modules per session (Discussed in Chapter 5 Section 5.1)
- Time allocated for each section of the class (Discussed in Chapter 5 Section 5.3)
- Methods used to grabs students' attention from the beginning (Discussed in Chapter 5 Section 5.3)
- Course content and the reason behind topics selection (Discussed in Chapter 5 Section 5.3)

- Evaluation method to determine the effectiveness of the program (Discussed in Chapter 5 Section 5.4)
- Involvement of the three I's (Intention, Interaction, and Introspection) (Discussed in Chapter 5 Section 5.5)

3.3 Develop

Moving to the next step, the Develop phase, the course is prepared according to the Design phase elements. This section focuses on PowerPoint slides preparation, dividing the course content into modules, developing modules, interactive and informative content preparation, and assessment preparation. By the end of the Develop chapter, the following notions are examined:

- Number of informative and interactive slides (Addressed in Chapter 6)
- Possibility for all the students to engage in the session's interactive parts (Addressed in Chapter 6 Section 6.1)
- Length and content of the evaluation method (Addressed in Chapter 6 Section 6.2)
- Validate the effectiveness using the assessment method (Addressed in Chapter 6 Section 6.2)
- Involvement of the three I's (Intention, Interaction, and Introspection) (Addressed in Chapter 6 Section 6.3)

3.4 Implement

The fourth step, Implementation, is to carry out the proposed training utilizing the information gathered in the last two phases. This phase includes three tasks, namely drafting, production, and evaluation [120]. Within this section, the emphasis is on introducing the course, starting the program, and collecting the students' assessments and feedback. By the end of this chapter, the following items are reviewed:

- Time and date of organizing the class (Covered in Chapter 7)
- Existing pilot run before the class and related feedbacks received (Covered in Chapter 7)
- Students' engagement level in the interactive parts of the class (Covered in Chapter 7)
- Number of students responded to the assessment process (Covered in Chapter 7)
- Involvement of the three I's (Intention, Interaction, and Introspection) (Covered in Chapter 7)

3.5 Evaluate

The final phase is Evaluation. This step is done throughout the implementation phase [120]. The evaluation method of this research is two-fold; pre/post-test method and knowledge rating of the students at the beginning and end of the class. By the end of this phase, results are collected and analyzed, the efficiency of the course is assessed, and the following concepts are addressed:

- Feedbacks received from the students (Covered in Chapter 8 Section 8.1 and 8.2)
- Students ability to grasp the content (Covered in Chapter 8)
- Process of gathering data related to effectiveness measurement (Covered in Chapter 8 Section 8.1 and 8.2)
- Process of determining the effectiveness of the project (Covered in Chapter 8 Section 8.1 and 8.2)
- Possible changes to the class before the actual run (Covered in Chapter 8)
- How is the clarity of instructions assessed? (Covered in Chapter 8)
- Involvement of the three I's (Intention, Interaction, and Introspection) (Covered in Chapter 8)

4. ADDIE model Step One: Analysis

In this section, the progress, findings, and analysis of the questionnaire and interview conducted to get a basic understanding of the current state of the students' cybersecurity awareness are discussed. These notable findings are used in the following chapters to identify the course structure and define the program's outline by charting down the required or unnecessary concepts to be covered by the course. Within this chapter, the research question of "what is the current state of the students' cybersecurity awareness level on different concepts of cybersecurity?" is thoroughly acknowledged. As research methods in this step, a survey and interviews were instrumented.

A questionnaire had been prepared in Persian language, and several school teachers and principals have been contacted to help with its distribution. The dispersal of the questionnaire was performed using Google Forms. A total of 616 responses were collected from Hormozgan state. In addition, an interview was organized with one of the high school principals in Hormozgan to acquire supplementary information on the topic. Complete questionnaire and interview questions are provided in Appendix 1 and 2 correspondingly for additional information.

According to data published on the Knoema website, 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 2017 in Hormozgan [121]. This sets the total population to approximately 124,000 students. The research by Robin Hill on the efficiency of sample size in Internet surveys is used to stress the efficiency of statistical representation [122]. The researcher emphasizes that for a 100,000 population size, a sample size of 384 is enough to represent the statistically significant results [122]. With this in mind, it is worth noting that the 616 answers collected from the questionnaire are more than enough to demonstrate statistical significance.

Here, obtained information on students' knowledge of cybersecurity's basic practices are reviewed. Based on the analysis, it can be concluded that the pupils lack knowledge on basic cybersecurity practices and online safety, and hence, they are vulnerable to different types of cyberattacks. The questionnaire was designed to capture student's existing knowledge on some cybersecurity awareness topics, including:

- clicking unknown links
- backups
- VPN security
- password security
- abuse of the unattended device
- phone antiviruses
- software update
- phishing attacks
- being hacked
- cyberbullying

4.1 Students' Current Knowledge

The first four questions were to capture the participants' gender allocation, age range, most used devices, and the daily hours spent surfing the Internet. Figure 8 indicates that 66.1% of the responses received were from the age group of 16-18 years old students; thus, it is decided to continue the survey analysis with more focus on this age range and develop a course content that is suitable for them.

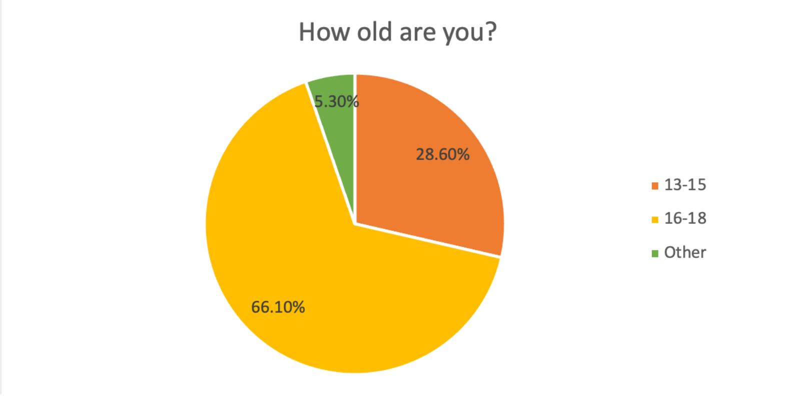


Figure 8. *Age distribution of all participants.*

Figures 9 and 10 specify the gender distribution of all the responders and students aged 16 to 18 years old. It can be seen that the ratio of the female are two-third of all responses while the gender dissemination of the age target group is more balances with 57% female and 43% male students.

Due to the shift of the focus group from students aged 13-18 to 16-18 years old students, from this point forward, the analysis, graphs, and figures of participants with the age range of 16-18 are elaborated.

Figure 11 represents the types of devices used by pupils to connect to the Internet. The

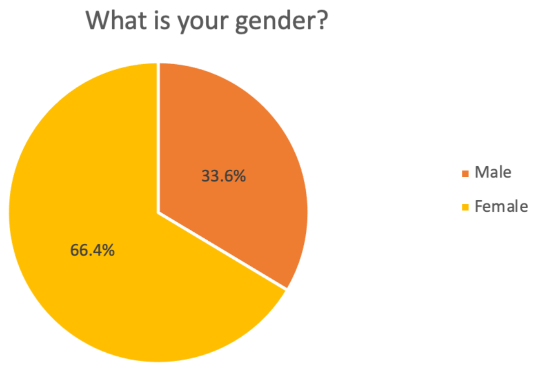


Figure 9. *Gender distribution of all participants.*

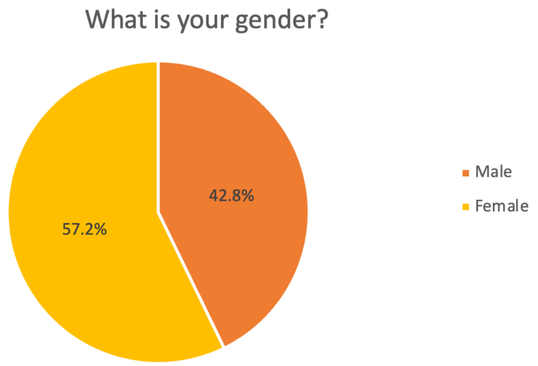


Figure 10. *Gender distribution of participants aged 16-18.*

responses indicate that cellphones are the primary devices used by the students, with more than 74% of usage. Figure 12 specifies that the amount of daily Internet usage by the 16 to 18 years old teenagers in Hormozgan is relatively high. Around 30% of the students surf the web 5 to 10 hours per day, and a total of 30.8% of the students are online for more than 10 hours daily. Thereby, using the two above-mentioned figures, it can be concluded that the majority of the course focus should be on mobile phone, their related security issues, and cyber hygiene.

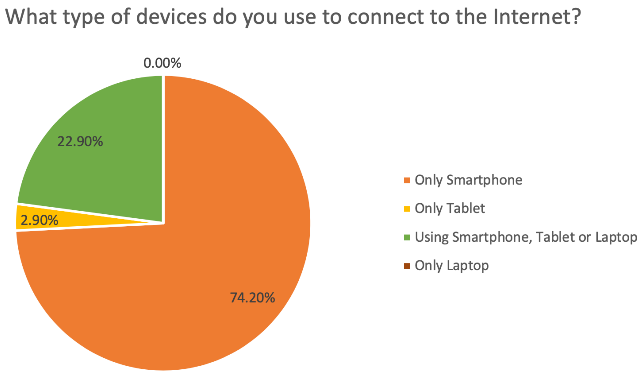


Figure 11. *Pupils' devices for connecting to the Internet.*

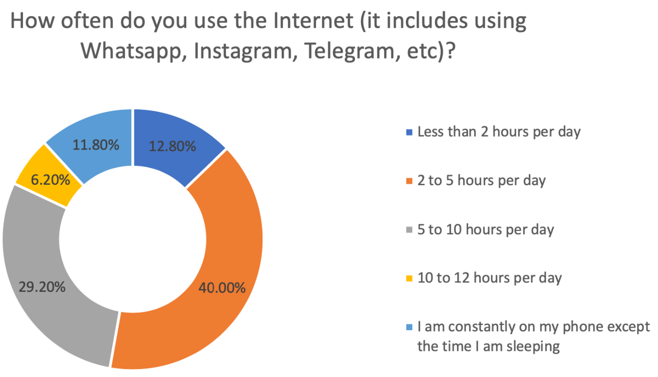


Figure 12. *Students' daily Internet usage.*

Figure 13 illustrates the most used phone applications. It can be seen that the most used applications are WhatsApp, Instagram, and Telegram, with 350, 169, and 55 responses, respectively. This brings a designated focus on the possible attacks that could threaten the students through these platforms. Here, it is safe to say that email phishing could not be addressed in Iran as email is relatively low, and people's main communication tools are the above-mentioned applications.

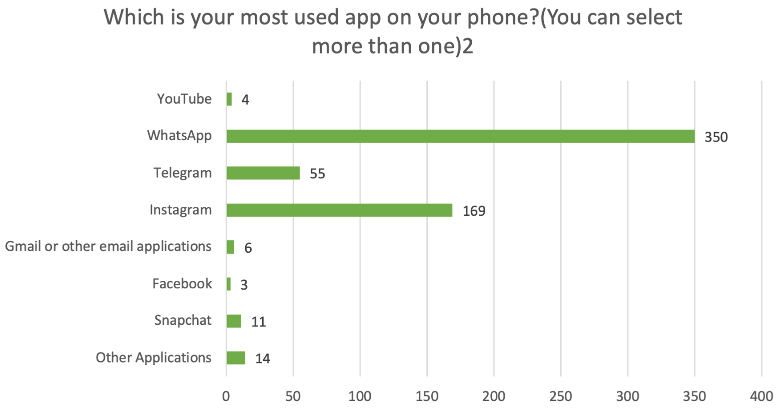


Figure 13. *Students' most frequently used applications.*

The next question analyses the students' willingness to click on unknown links. As it is shown in Figure 14, it is a concern that around 56% of the pupils could be victims of phishing or malware attacks as they would click links based on the caption. Meanwhile, 5.7 percent of the students click on the links without any hesitation. Therefore, a course section is required on link trust and making sure only safe links and websites are visited.

Figure 15 presents the knowledge and willingness to perform a backup of the data stored on devices. It is evident that 62.4 percent of the students do not know how to back up their information or do not appreciate the value of the information stored on their devices, and they do not have the eagerness to store backups of their data. Hence, a general explanation

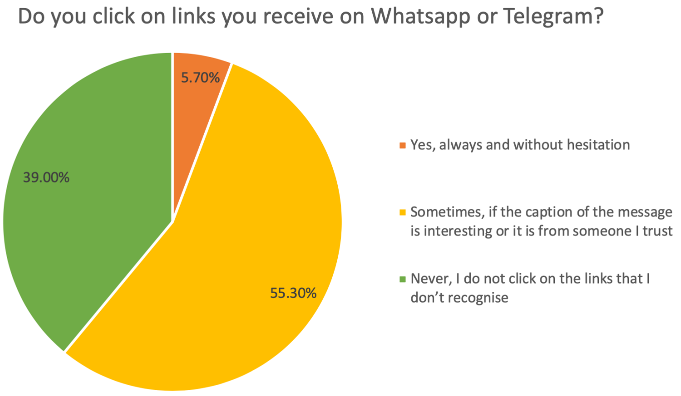


Figure 14. *Students' willingness to click on unknown links.*

on why backups are important with example scenarios of the negative impacts of when data is lost and cannot be retrieved could be added as a course section.

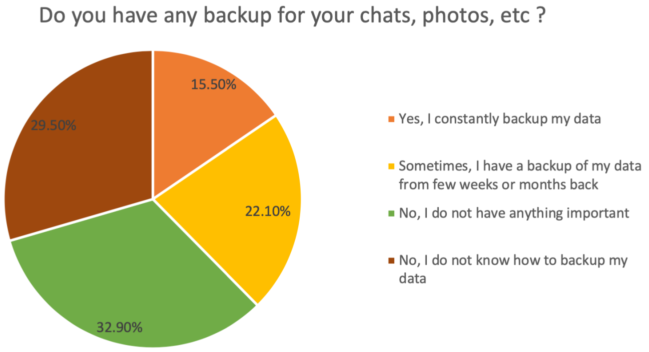


Figure 15. *Backups performed by the pupils.*

The following five questions' point of convergence is about VPN security. The first question is manifested in Figure 16 which asks about the usage regularity of the VPNs. Around 3.9% of the students have their VPNs always switched on, and 58.7% of the total respondents are using VPN for at least one application, and they switch it on depending on the need.

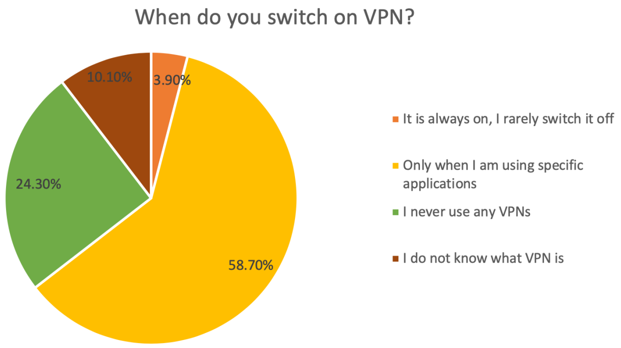


Figure 16. *Students' VPN usage regularity.*

The next question is designed to understand which applications need VPN to access. Figure 17 specifies that students mostly use VPNs to access Telegram, YouTube, and Snapchat applications. Moreover, Figure 18 illustrates that majority of VPN users are using free versions of the applications. It can pinpoint that the security of VPN is not considered while using.

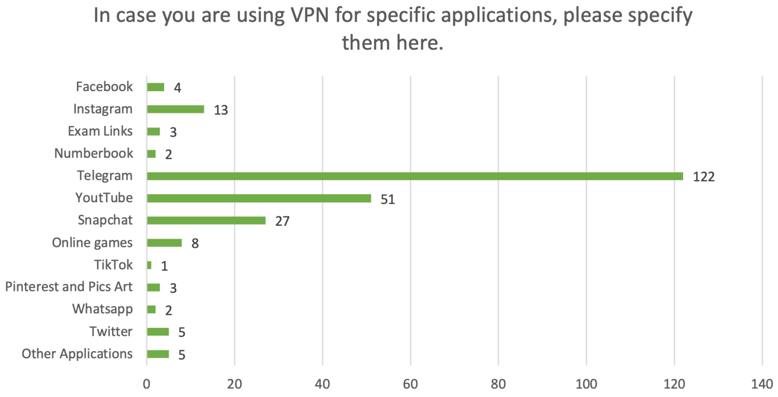


Figure 17. *Applications that students use to connect to the internet through a VPN.*

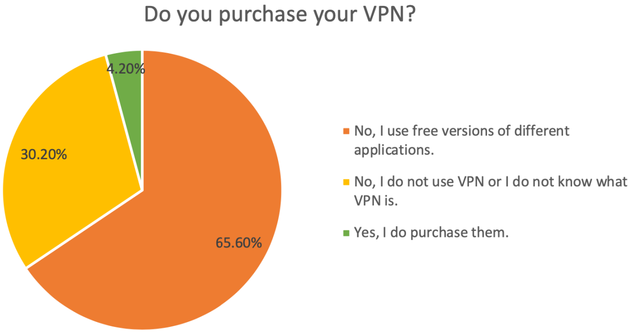


Figure 18. *Purchased VPNs by the pupils.*

The last two questions are to capture their level of knowledge on the concept of VPN security. Based on Figure 19, only around 45% of the students claimed that they know completely what VPN security is, or their knowledge is limited to some readings. However, when asked to explain the information they have on the VPN security, it showed that majority only know what VPNs are used for. The following are examples of answers gathered:

- I use VPNs to access applications that are filtered in Iran
- I use it for accessing Snapchat and Telegram
- I just know that foreign applications need VPN to start
- It is something like a backdoor to access applications that are filtered in Iran
- It is good for increase of security and access to the web
- VPNs can copy the phone's information; it is used to access the specific application, it drops the Internet speed.

- It is an application used to grant access to other application which will not open or have a minimal speed.
- It changes my location so that I can access the applications
- It is an application that connects us to the Internet of other countries
- The VPN developers can access our data

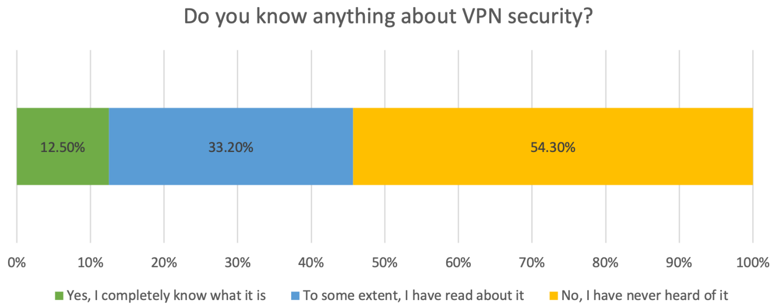


Figure 19. *Knowledge of the students on VPN security.*

Nevertheless, the succeeding six questions are designed to understand the pupils' knowledge and practice of passphrase security. According to Figure 20, over 80% of the responders claim to know basic to advance knowledge on the concept. Figure 21 illustrates that 173 students believe that a combination of random numbers, letters, and characters is the characteristics of a strong password. On the other hand, 105 responders identified a strong passphrase as a set of characters containing their name, birthday, and phone number. It is easy to remember, and 117 responders select their password as a phrase to remember.

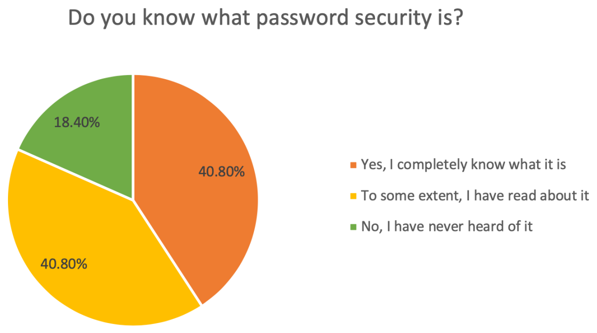


Figure 20. *Knowledge of the students on password security.*

The next question asked students to explain password security in their own words. The majority of the responses showed that they use their names, birth dates, and phone numbers as their passwords. They explained the reason behind this selection is the easy-to-remember characteristic of the passphrase. However, the fact that some of the responders populated their passwords through the form was alarming. Students could benefit from more information on password security when selecting and sharing passphrases.

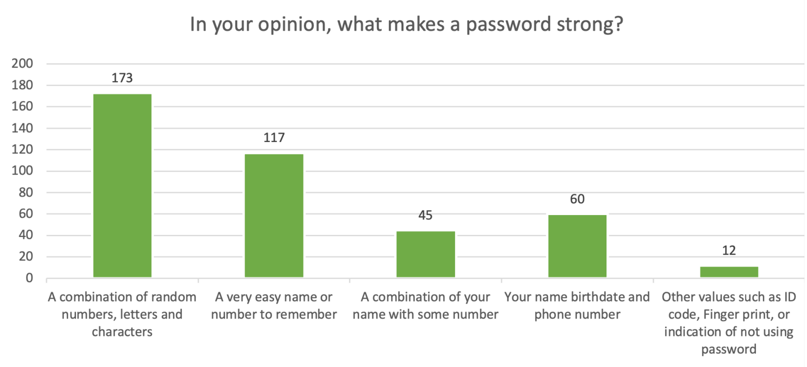


Figure 21. *Knowledge of the students on selection of strong password.*

In the meantime, Figures 22, 23 and 24 illustrate the students' awareness of the concept of password sharing. Firstly they have been asked if they have shared their passwords with anyone before, followed by a trick question to know if they have shared the password in case of necessity and finally if they have changed their passphrase afterward.

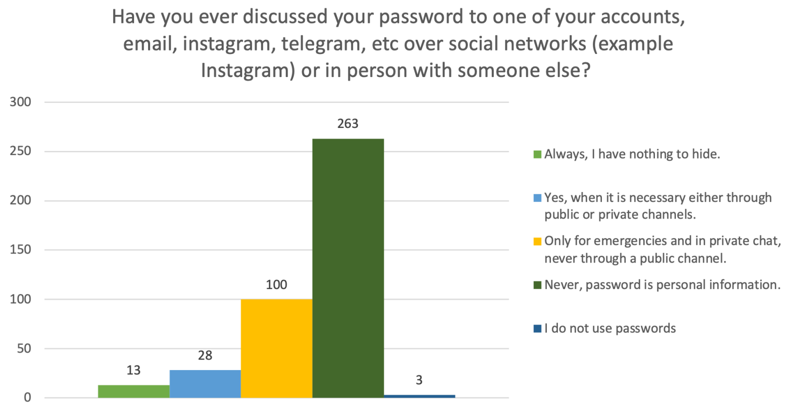


Figure 22. *History of pupils sharing passwords with others.*

Interestingly, amongst 263 students who responded that they never discussed their passwords with someone else, 60 of them asked for help fixing an issue and shared their passwords along the way. 47 responded that they did not change their passwords afterward, which means there still are many people, including technicians, friends of family members, who know their passphrase.

Figure 22 also specifies that 28 pupils share their passwords on public or private channels when necessary, which shows a lack of awareness. Figure 24 also presents that around 50% of the responders do not change their passwords once shared, either because they do not know how to change the password or do not think it is necessary.

Moreover, to acknowledge the students' awareness level on the concept of abusing unattended devices, the question shown in Figure 25 has been asked. Around 22% of the

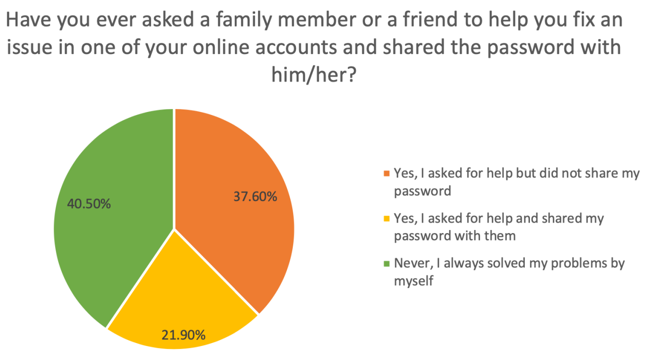


Figure 23. *History of students asking others for help regarding fixing an online issue.*

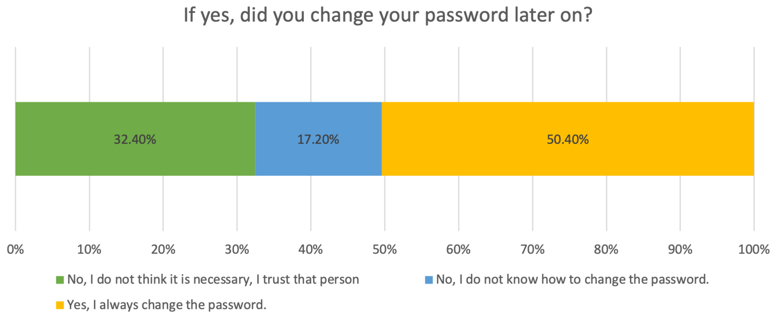


Figure 24. *History of students changing their password after request for help regarding fixing an online issue.*

respondents mentioned that they do not have anything important or confidential to be exploited. In contrast, approximately 35% of the responders specified that there is a possibility of their phones and social media being abused if they are left unattended. In this regard, it is understandable that students did not understand the concept of confidentiality as expected. Per discussions on Iran's cultural differences in Section 2.7 of Chapter 2, photos stored on devices are considered confidential. While, it seems that students did not consider social values while responding to this question.

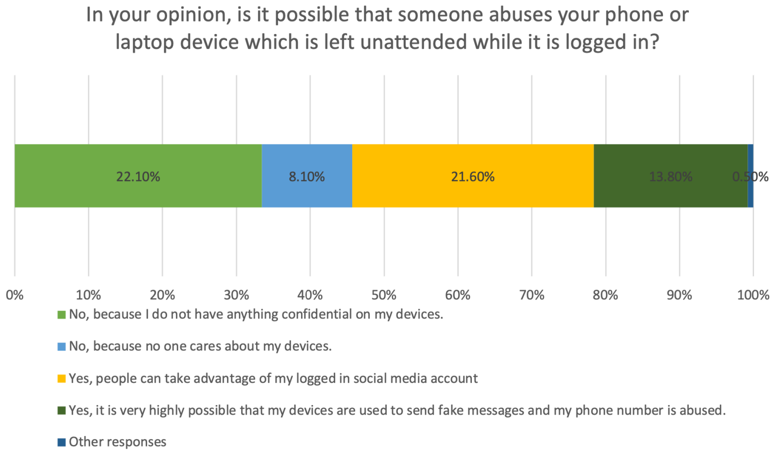


Figure 25. *Students' thoughts on the possibility of unattended devices to be abused.*

Furthermore, Figure 26 presents that only 17% of total responders know about phone antiviruses and have them installed on their phone devices. 31.9% of the students think it is not an essential application. Meanwhile, approximately 50% of the students do not know that phone antiviruses exist or they do not know if it is installed on their devices or not. This percentage highlights the need for a section of the course to educate students on antiviruses' usage and benefits.

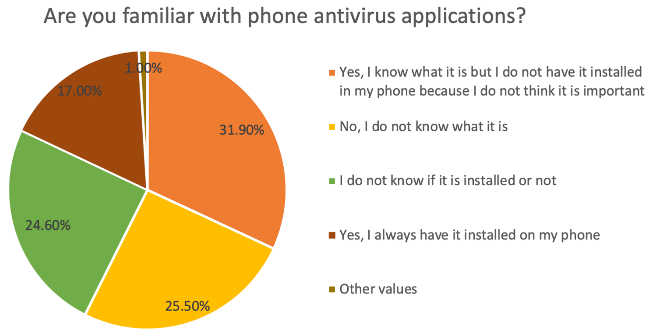


Figure 26. *Students' familiarity with phone antivirus applications.*

The survey results shown in Figure 27 are promising. The graph depicts the students' understanding of the concept of software updates. It must be pointed out that 76.7% of the students either have their automatic updates activated or immediately install software updates manually. The reason may be many pop-ups and notifications show up on the screen once a software update is requested. Thus, due to the learners' relatively high update installations habit, this section is emitted once the course is being designed.

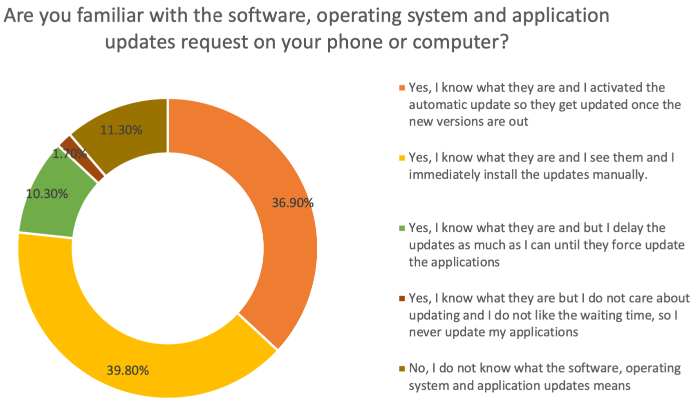


Figure 27. *Students' familiarity with software updates.*

The next two questions are asked to obtain the knowledge level of students on phishing attacks. Figure 28 represents that approximately 60% of the pupils declared that they have never heard of this type of attack. Amongst the remaining respondents who claimed they know what phishing attacks are, there were few interesting explanations on their understanding of what this type of attack is:

- It is also called hacking; it means your photos, videos, and bank information are stolen from your device, and they are used to threaten you.
- They steal money from your account through gaming and gambling websites.
- I have received a link on WhatsApp, and then I was asked to call a number. After calling, I was a victim of a phishing attack, and after that, I have never clicked on unknown links again.
- Some time you receive links to gain more Instagram followers, but once you enter your account ID, email or password, that account will be gone.
- Stealing information through Internet, Bluetooth, or email.
- Attack on phone, tablet, or laptops which contain personal information.
- They empty your bank account.
- Phishing means an attempt to get information such as user ID, password, and bank information.
- Some apps will be secretly installed on a person's phone and can access all the stored data.
- Sometimes I receive messages that if you have received a message from a specific number, do not respond.
- unauthorized access to your devices to access your information.

According to the above list, only a few responders commented on their understanding of the phishing concept correctly. Many of them associate phishing attacks with attacks on their bank account. Hence, this subtopic is marked to be added to the course curriculum.

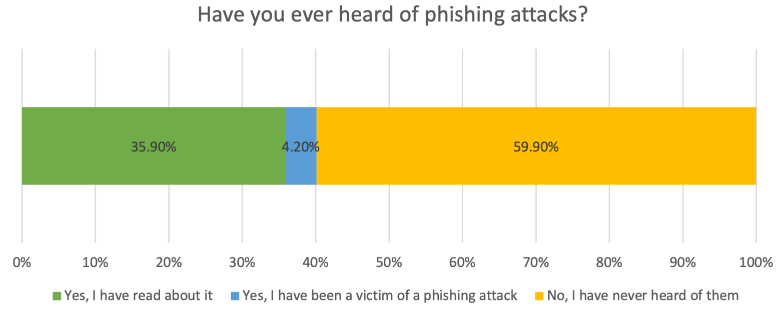


Figure 28. *Students' familiarity with phishing attacks.*

Furthermore, as shown in Figure 29, more than 92% of the students have never been victims of a cyber-attack. Amongst those who responded "yes" to previous encounters with cyberattacks, they provided the following explanations on the events:

- My computer was infected by viruses, none of the software was working so we needed to format the computer.
- I received a message to change my password, so I was logged out of all my accounts.

- Someone hacked my account and sent messages to others.
- My computer has been infected by a virus multiple times, but no information was stolen.
- My mom shopped online, and there was money deducting from her account monthly without her consent.

One assumption on the figures received is that the students have no idea what constitutes a cyber-attack. Perhaps they only consider financial or data theft-related attacks as cyber-attack and not malware infection. Accordingly, if the topic is discussed in the class, more information could be gained to understand what events are considered cyber attacks.

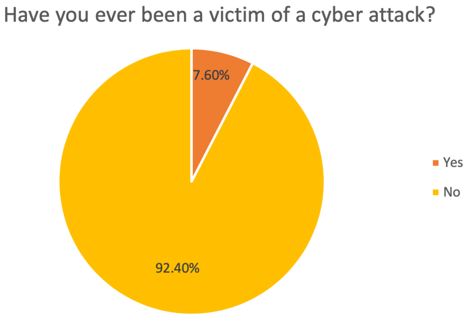


Figure 29. *Student's previous experience with being a victim of cyber attack.*

Meanwhile, when the pupils were asked if they have ever encountered hacking, 7.8% of the responses claimed that they had been a victim before, and 26.3% responded that they know someone who faced this situation at some point in their lives. These values suggest a need to teach students the steps to take in case they have been hacked. This information is represented in Figure 30.

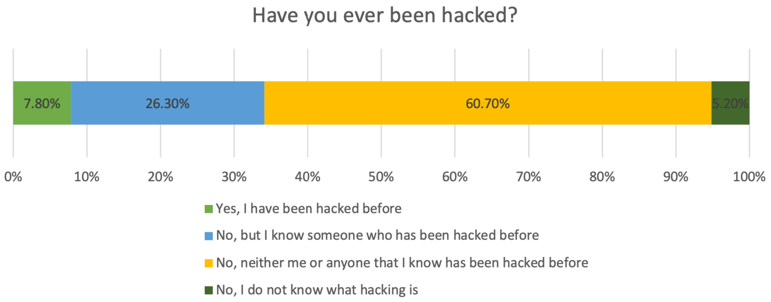


Figure 30. *Student's previous experience with being hacked.*

Figures 31 and 32 illustrates the awareness level of the students on the concept of cyber-bullying. It can be seen in Figure 31 that a total of 42.5% of the students declared their familiarity with cyberbullying . Only 3.7% of the total pupils noted that they are aware of cyberbullying and had been a victim of it. On the other hand, Figure 32 represents that 26.8% of the students received negative comments and language through social media.

This indicates that more than 3.7% of the students have been cyberbullied while they do not know what the concept is about. They were unaware of the negative impacts these occurrences could have on their physical or psychological well-being. However, due to a small percentage of the student being affected, it has been decided not to cover this topic in the program.

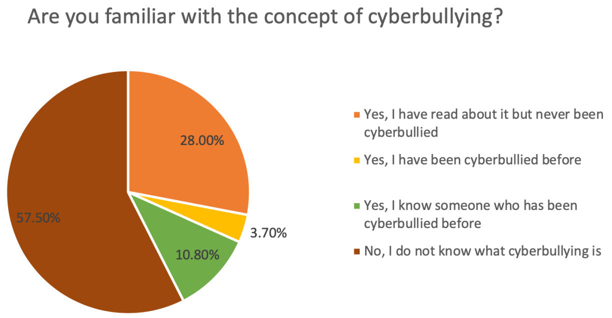


Figure 31. *Student's awareness level on cyberbullying.*

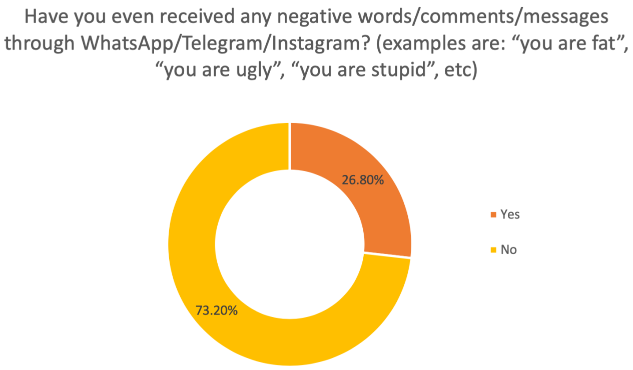


Figure 32. *Students' previous experience with cyberbullying.*

Over and above the mentioned cybersecurity concepts, Figure 33 indicates that, unfortunately, only 5.9% of the responders affirmed that they had received cybersecurity training before. This designates the lack of cybersecurity awareness training programs in Iran, Hormozgan for 16-18 years old students. When asked for comments from those who have taken a related program before, only one comment was received, described as "the topics were about how to use a virtual environment, how long we should spend online, and what actions to take when we are facing a cyber attack."

4.2 Content to be Taught

This section is to complete on the topic selection process of the proposed program. Based on the analysis shown in the above section, it has been decided that the program includes the following topics:

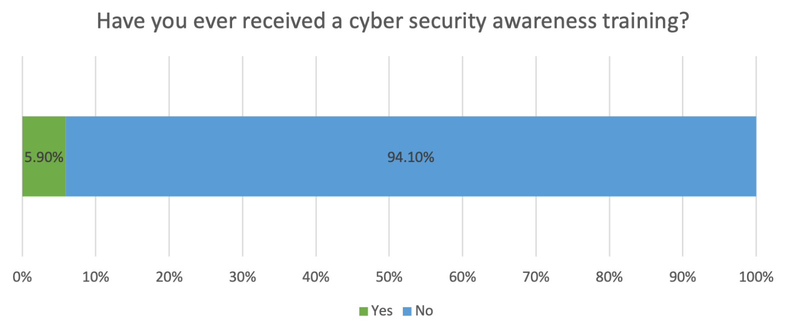


Figure 33. *Students' existing in attending a cybersecurity awareness training.*

- General concepts of phone security
- Security of unknown links click in mobile application
- Backups
- VPN security
- Password security
- Unattended Devices
- Antivirus applications
- Phishing attacks

4.3 Culture of Education in Iran

During the interview, the school principal mentioned that before the world pandemic and shifting to remote studies, "majority of the classes were organized traditionally." She elaborated that the conventional approach involves teachers explaining concepts and students memorizing them. Some classes like Mathematics, students might be asked to come to the board and solve a problem. But humanitarian or other courses follow the traditional teacher-oriented teaching method.

In addition, the principal also mentioned the following to be the new approaches to teaching starting distance learning:

- Using Moodle (BigBlueButton) to organize classes
- Recording a voice message or a video clip explaining the class and sharing with the students through WhatsApp
- Uploading educational videos found online on the Moodle platform
- For exams, video calls take place over WhatsApp applications so that the teachers can ask students the questions in mind.
- Another method is called reverse-learning, in which teachers ask the students to go through specific chapters of the book and contact the teacher if they have any

questions or need more clarifications.

Despite the limitation that one interview is not enough to conclude the culture of education, the analysis suggest that the students would not have the courage to participate in class activities due to not being accustomed with interactive classes. Also, lack of class presentations and group activities lead students to lean towards being inactive in classes and loose the willingness to participate in class discussions. Therefore, as this thesis is planning to propose an interactive class, the training would follow a new approach and it would be different from normal classes in Hormozgan province.

4.4 Online Environment

Teaching methods are essential in ensuring the pass of knowledge into the learners. Some methodologies are teacher-centered that achieve less result, while the pupil-centered methodologies tend to be more productive [123]. One of the questions in the questionnaire asked the students to select their preferred learning method. The results are introduced in Figure 34, and it specifies that they prefer lectures over any other learning method, followed by learning through videos.

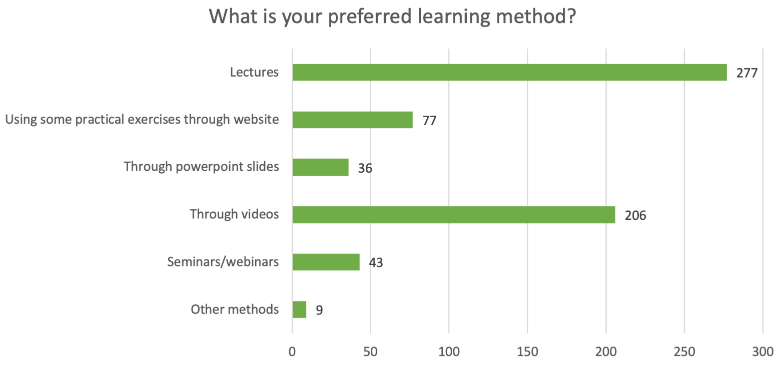


Figure 34. *Student's preferred learning method.*

Due to the current situation, no physical face-to-face classes are taken place in Iran at the time of conducting this research. Hence, the best substitution for the lecture teaching method is online classrooms organized through Skype, Zoom, Google Classroom, or other applications that provide the experience close to interactive in-person classes. However, the majority of the mentioned platforms were censored in Iran and therefore pointless to use. Amongst Iranian online streaming platforms, Skyroom could be mentioned [124]. This platform is very similar to Skype and very advantageous when organizing online classes and webinars. During the interview with the school principal, when asked about the most suitable platform for holding the training, she suggested the use of the Moodle platform. This platform is translated into Persian and therefore beneficial for this scenario.

As of technical specifications, other than a phone (or a personal computer or a tablet), Internet connection, microphone, and a speaker no additional equipment is needed. A screenshot of the platform used is shown in Figure 35.

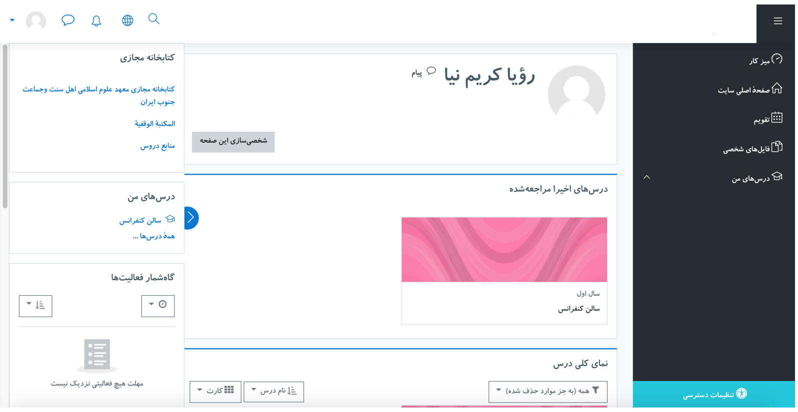


Figure 35. *Screenshot of the Persian Moodle platform.*

4.5 Desired Learning Outcomes

The desired learning outcome of this training is to meet the first three stages of Bloom's taxonomy. It is planned for the students to remember, understand and apply all the discussed topics. Table 3 demonstrates the expected learning objective of the class.

Table 3. *Expected Learning Objective*

Topic	**Learning Objective**
General concepts of cybersecurity	Students will 1. understand the definition of cybersecurity and its importance 2. demonstrate their understanding of phone security. 3. apply the actions discussed to increase their phone security

Continues...

Table 3 – *Continues...*

Topic	**Learning Objective**
Security of unknown links click in mobile application	Students will 1. understand the ways to receive an unknown link 2. comprehend the first principle and action when receiving a link 3. differentiate better between fake and real received messages 4. introduced to the ways they can check a short link 5. apply the actions discussed to increase their phone security
Backups	Students will 1. understand the definition of backups, its importance, and benefits 2. identify the lack of it on their devices (if any) 3. learn how to activate the backups for different applications 4. implement the use of backups for their mobile devices and applications
VPN security	Students will 1. understand the definition of VPN, its advantages and disadvantages 2. identify trusted and untrusted VPNs using the introduced tools 3. be given a list of trusted VPNs to install 4. implement the tools when installing a new VPN
Password security	Students will 1. acknowledge that if personal information is used in a password, it will be easy to guess 2. identify a strong password from a weak password 3. apply the tools when choosing a new password

Continues...

Table 3 – *Continues...*

Topic	**Learning Objective**
Unattended devices	Students will 1. understand the drawbacks of leaving their devices unattended 2. be familiarized with some case studies of misusing unattended devices 3. not leave their devices unattended
Antivirus applications	Students will 1. understand the benefits of installing an antivirus 2. be familiarized with trusted and most rated antiviruses 3. use antivirus application on their devices
Phishing attacks	Students will 1. understand what phishing attacks are 2. identify measures to prevent a phishing attack 3. be familiarized with some case studies of phishing attacks 4. take actions to prevent such attacks

5. ADDIE model Step Two: Design

In the previous chapter, the conclusion was that there is a significant need to educate high school students aged 16 to 18 years old in Iran, Hormozgan, due to the shortage of knowledge on the basic cybersecurity concepts. To ensure the course's effectiveness, Bloom's taxonomy has been taken into consideration to provide the students with the Apply level of the theory [125]. This chapter aims to design a training program that provide the students with information, skills, and encouragement to apply the basic cybersecurity concepts in their lives, with respect to the culture of their society.

As discussed in the previous chapter, this course is designed to cover the following cybersecurity concepts:

- General concepts of phone security
- Security of unknown links click in mobile application
- Backups; benefits and how to implement for most used applications
- VPN security; do and don'ts
- Password security; do and don'ts
- Unattended Devices; what could go wrong and how to prevent
- Antivirus applications; benefits and how to use
- Phishing attacks; how to prevent and after actions

Learning objectives and communication tools are discussed in Sections 4.5 and 4.4 of Chapter 4. By the end of this chapter, the general program description, course content, helping tools, and course evaluation methods are addressed. Hence, the research question "What is the content of the newly designed course?" is answered in this chapter.

5.1 General Program Description

The course is called "Introduction to Cyberspace Security," and is taught to 16 to 18 years old students in Iran, Hormozgan. The program is completed in two sessions of 1.5 hours each and with a class with a minimum of 20 students. The medium of the instruction is Persian, and the class is organized using the BigBlueButton tool. The students are able to register for the class by contacting authorities in the schools they are enrolled in.

This course ensures the increase of the students' awareness level and acts as a motivation pushing them to practice the concepts learned within this course.

5.2 Helping Tools and Students' Engagement

The first helping tool is the use of Google Slides. This application is used to prepare teaching slides. Another related tool is google form which is utilized for publishing pre-test and post-test questions amongst the students.

One of the challenges in online classrooms for the instructors is how to increase interactiveness in class [126]. This means that innovative techniques and various resources ought to be used in the learning process [126]. One of the tools utilized for increasing the students' engagement in the class is an online tool called Wooclap [127]. This tool is used when the instructor is planning to ask a question addressed to all the students. Hence, instead of asking for volunteers to speak, many attendees may have the courage to type their thoughts. Another action for increasing the students' engagement in class is designing short games. For the first session, a game of Guessing Password is planned. More details on the game could be found in Chapter 6 Section 6.1 of the thesis.

5.3 Course outline

The course is designed so that during the first lecture, five modules and during the second session, four modules are discussed. Session one focuses on the introduction to Cybersecurity, Phone, VPN, Password Security, and Unknown Links Click. Meanwhile, the second lecture consists of Unattended Devices, Backups, Antivirus, and Phishing Attacks. Tables 4 and 5 are the predicted time allocation of each section of the class.

Table 4. *Time Distribution of First Session*

Topic	**Allocated time**
Course and Instructor's introduction and Course Outline	10 minuets
Introduction to cybersecurity	15 minuets
Phone Security	20 minuets
VPN Security	20 minuets
Password Security	20 minuets
Unknown Links Click	20 minuets

Continues...

Table 4 – *Continues...*

Topic	**Allocated time**
What have you learned session	10 minuets

Table 5. *Time Distribution of Second Session*

Topic	**Allocated time**
Course outline	5 minuets
Unattended Devices	20 minuets
Backups	20 minuets
Antivirus	20 minuets
Phishing Attacks	20 minuets
Question and Answer	20 minuets

To ensure the course grabs students' attention from the beginning the method of Storytelling is used. This method has been introduced as an effective way of teaching in which students' attention would be caught at first and an item to remember when thinking of the class events [128]. As a result, a relevant and adequately alarming story is told to ensure that the students are committed to class and that they pay attention.

Lecture 1

This section contains basic definitions and information on the definition of cybersecurity, its importance and principles, aiming to reach the Understand level of Bloom's taxonomy is reached [125]. Furthermore, the security of VPNs and passwords are discussed. By the end of the session, it is expected that the students have basic knowledge of what VPN is and the security issues of free VPNs. They are also equipped with notes on the proper selection of passwords. To ensure the Apply level of Bloom's theory is touched, a game of "Can I guess your password" is played.

An outline of the information provided in the course is as follow:

- What is cybersecurity?
- Why is it important?
- What is the outcome of this course?
- Why is phone security important?
- What is confidential on your phone?

- How to know if the link we are clicking is safe?
- What VPN does?
- How to increase the security when using VPN?
- Can I guess your password game?
- What is a good password?
- Why is it important to change your password?
- How to change your passwords?

Lecture 2

The emphasis of this section is on four topics. 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 ensures that students understand how to install them; consequently, it ensures that they have a general understanding of what to do if they have been hacked.

This section attempts to initiate Apply level of the theory by providing examples of what-could-go-wrong when teaching the Unattended Devices, Backups and Antivirus concepts. Whereas, for phishing Attacks topic, the focus is on the Understand level of Bloom's theory.

- Locate phone and remote wipe apps
- How to perform backup on WhatsApp and Telegram?
- How to secure your Instagram account so you will not be hacked easily?
- Why are antivirus applications important?
- How to install antivirus applications
- What to do if you have been hacked?

5.4 Evaluation Method

Ensuring and evaluating the programs effectiveness is critical. The pre-test post-test approach is one way to assess the instructional program's effectiveness [129]. When majority of the students responded to both tests, a baseline can be established for comparison [129]. However, there are certain unreliability issues with this approach. Since the post-tests are released immediately after the lessons, there are aspects of timing and attention given to the students' class. Since there is not much time passed, the students are more likely to remember the content. In addition to enforcing the pre-test post-test methodology, two questions are posed during the class. The first question is at the beginning of the class, asking the students to rate their current cybersecurity knowledge on a scale of one to one hundred. The second question is asked at the end of the lesson, in which they give another appraisal of their knowledge and to name one thing they have learned. The author claims that the tests listed above would aid in validating the course's effectiveness.

5.5 Cultural Aspects of Design Phase

There are some taboo topics discussed in Section 2.7 of Chapter 2 on the cultural differences between Iran and the West. Among them are sexual issues. When creating the course, the author interacted with the chosen school principal directly to validate the program's material.

On the topic of content selection, this chapter uses the information gathered in Chapter 2 and 4 to eliminate topics such as Public WiFi Connections, and E-mail Security, while including topics like VPN Security.

Another cultural aspect taken into consideration was the introduction of the used Wooclap tool [127]. This website, similar to the majority of English language and popular websites, used cookies. As mentioned in Section 2.7 of the Chapter 2, Iranians are not familiarised with seeing Cookies agreement pop-ups. Therefore, a small tutorial is needed to familiarise the students with the Wooclap websites and inform them of clicking on the agree button when the agreement pop-up is viewed.

Another point to consider is the Internet speed in the rural area of Iran is very low [130]. Currently, there are 256 villages in Hormozgan which are reported not having Internet connectivity or having a very limited bandwidth [130]. Therefore, there might be Internet disconnectivity for the students attending the class from small villages in Hormozgan. According to the interviewed school principal, there were days that we ought to cancel classes because the Internet speed is significantly low. During those days, it is not possible to stream on the BigBlueButton platform, and we switch to the WhatsApp application for teaching. In case this issue is risen during the implementation phase, the author plans to record a video, explaining and introducing the content with the slides shown side by side.

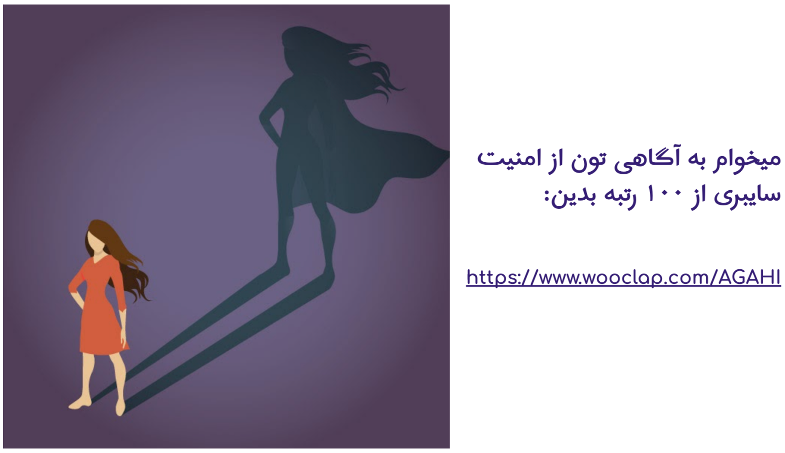
6. ADDIE model Step Three: Development

This chapter focuses on the development of the content discussed in the previous chapter. Alongside the slides' preparation, two pre-test and post-test google forms were inclined to be distributed before and after the training. Meanwhile, a total of 28 Google Slides were prepared in Persian for the session. Screenshots of all the slides are attached to Appendix 3 for reference. Unfortunately, due to time limitations, the author could only develop and execute the program's first session.

6.1 Session Development

The first slide of the class is for introducing the trainer, followed by a cybersecurity incident affecting a 19-year-old girl in Iran. The story talked about how the girl's phone was hacked in a gathering and the consequences she had to face due to the incident [131]. The story was published on the persianv.com news website [131].

The next slide in the course focuses on defining cybersecurity and reasons of its importance, followed by the interactive question that asked them to visit the link and rate their current cybersecurity knowledge from one to hundred. This slide, also, provides the possibility for all the students to engage in the class. Figure 36 illustrates the interactive slide, requesting students to evaluate their knowledge.

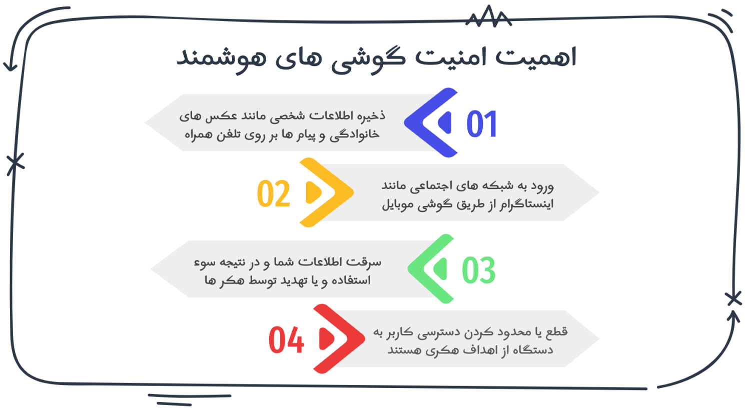


میخوام به آگاهی تون از امنیت
سایبری از ۱۰۰ رتبه بدین:

https://www.wooclap.com/AGAHI

Figure 36. *Screenshot of the slide asking students to rate their initial knowledge on cybersecurity.*

The consequent 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. Afterward, 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 agitate about phone security. Figure 37 exhibits the slide on the importance of phone security.



اهمیت امنیت گوشی های هوشمند

01 ذخیره اطلاعات شخصی مانند عکس های خانوادگی و پیام ها بر روی تلفن همراه

02 ورود به شبکه های اجتماعی مانند اینستاگرام از طریق گوشی موبایل

03 سرقت اطلاعات شما و در نتیجه سوء استفاده و یا تهدید توسط هکر ها

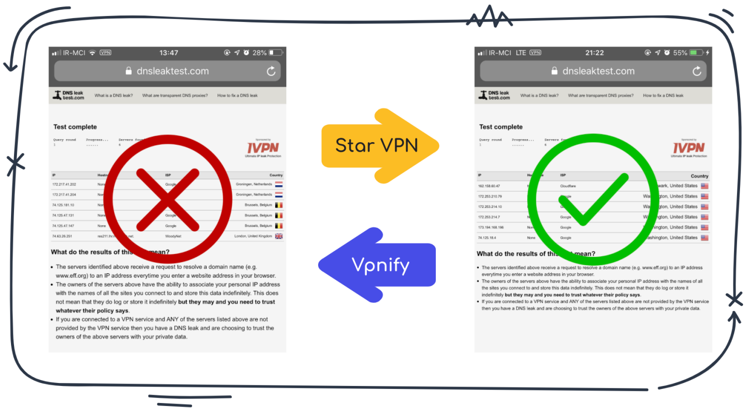
04 قطع یا محدود کردن دسترسی کاربر به دستگاه از اهداف هکری هستند

Figure 37. *Screenshot of the slide on the importance of phone security.*

The following three slides 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 activate remote phone formatting were provided. Additionally, several trusted antivirus applications are shared with them.

VPN security is the topic to discuss further. 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 the students to test the VPNs' security they are using. The websites 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 application's name. That information has been exploited, and all the mentioned VPNs were tested against the websites mentioned earlier. Unfortunately, many of the VPNs were not secured. Amongst those, Vpnify and Star VPN were selected to demonstrate secure and unsecured VPNs. Figure 38 portrays the slide discussed in class. During this discussion, the students are asked to switch on the installed VPN and check the websites mentioned above. Later on, they are introduced to a few reliable VPNs and encouraged to install them in order to improve their security.

The third topic discussed were the dangers that clicking on unknown links brings. One of



IR-MCI VPN 13:47 28%

dnsleaktest.com

DNS leak test.com What is a DNS leak? What are transparent DNS proxies? How to fix a DNS leak

Test complete

Query round 1 Progress... ...... Servers fou 6

Sponsored by IVPN Ultimate IP leak Protection

IP	Hostn	ISP	Country
172.217.41.202	None	Google	Groningen, Netherlands
172.217.41.204	Non		Groningen, Netherlands
74.125.181.10	Non		Brussels, Belgium
74.125.47.131	None	Google	Brussels, Belgium
74.125.47.147	None	Google	Brussels, Belgium
74.63.26.251	res211.lhr.r net.	WoodyNet	London, United Kingdom

What do the results of this mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address everytime you enter a website address in your browser.
- The owners of the servers above have the ability to associate your personal IP address with the names of all the sites you connect to and store this data indefinitely. This does not mean that they do log or store it indefinitely **but they may and you need to trust whatever their policy says**.
- If you are connected to a VPN service and ANY of the servers listed above are not provided by the VPN service then you have a DNS leak and are choosing to trust the owners of the above servers with your private data.

IR-MCI LTE VPN 21:22 55%

dnsleaktest.com

DNS leak test.com What is a DNS leak? What are transparent DNS proxies? How to fix a DNS leak

Test complete

Query round 1 Progress... ...... Servers fo 6

Sponsored by IVPN Ultimate IP leak Protection

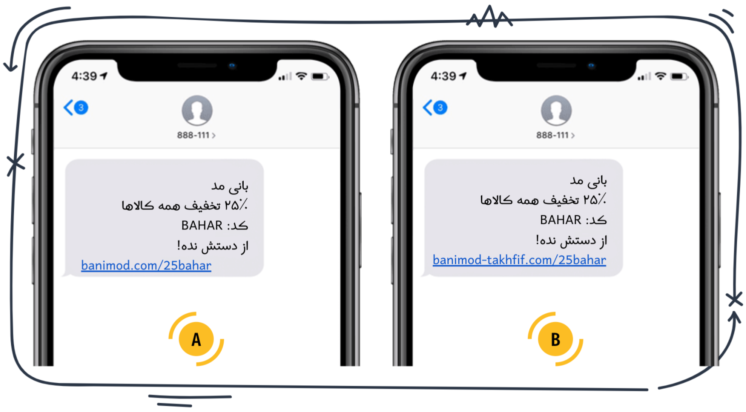
IP	Ho e	ISP	Country
162.158.60.47	N	Cloudflare	wark, United States
172.253.210.79		ogle	Wa gton, United States
172.253.214.10		G	Wa gton, United States
172.253.214.7	N	Google	W ngton, United States
173.194.168.196	Non	Google	hington, United States
74.125.18.4	None	Google	ashington, United States

What do the results of this mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address everytime you enter a website address in your browser.
- The owners of the servers above have the ability to associate your personal IP address with the names of all the sites you connect to and store this data indefinitely. This does not mean that they do log or store it indefinitely **but they may and you need to trust whatever their policy says**.
- If you are connected to a VPN service and ANY of the servers listed above are not provided by the VPN service then you have a DNS leak and are choosing to trust the owners of the above servers with your private data.

Figure 38. *Screenshot of the slide demonstrating secure and unsecure VPNs.*

the main focus points in class was encouraging the students to read and think about the necessity of accessing the link before they click. Figure 39 elucidates an example shown in class of two SMS messages received, and the students are asked to guess which of the links are actual and fake. To help the student differentiate between a fake and an original link in the future, they are introduced to Google's Transparency Report platform [132]. 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 the redirected websites.



4:39

888-111 >

بانی مد
۲۵٪ تخفیف همه کالاها
کد: BAHAR
از دستش نده!
banimod.com/25bahar

A

4:39

888-111 >

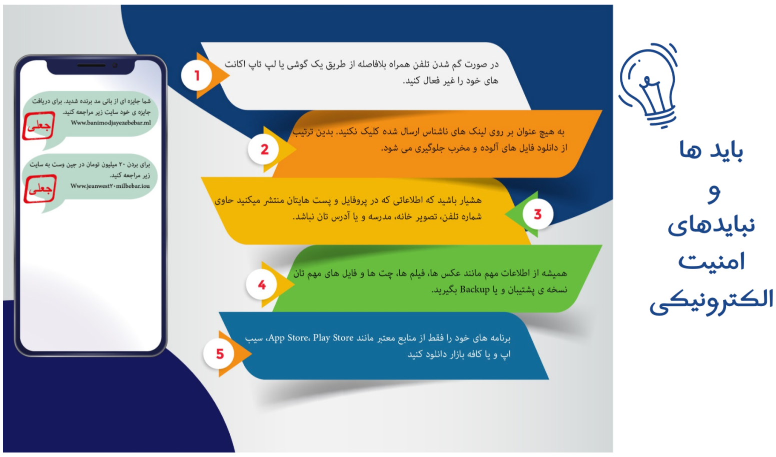
بانی مد
۲۵٪ تخفیف همه کالاها
کد: BAHAR
از دستش نده!
banimod-takhfif.com/25bahar

B

Figure 39. *Screenshot of two SMSs received and students are required to identify the real SMS.*

The last discussion of the training expounded around password security. Firstly, the Password Guessing Game is played by asking for one volunteer in the class. The volunteer was inquired with some basic questions such as birthday and phone number while the trainer would attempt to guess the password. Moreover, the students are familiarised with the *https://haveibeenpwned.com/Passwords* website to test the phrases they have in mind before the password selection and changing their passwords immediately if they are compromised.

Towards the end of the class, Figure 40 is displayed. It contains a summary of the course so that a revision would take place and the content adheres. Finally, another Wooclap link is shared with the students, asking them to name an item they have learned today and giving their cybersecurity knowledge another rating.



باید ها
و
نبایدهای
امنیت
الکترونیکی

1 در صورت گم شدن تلفن همراه بلافاصله از طریق یک گوشی یا لپ تاپ اکانت های خود را غیر فعال کنید.

2 به هیچ عنوان بر روی لینک های ناشناس ارسال شده کلیک نکنید. بدین ترتیب از دانلود فایل های آلوده و مخرب جلوگیری می شود.

3 هشیار باشید که اطلاعاتی که در پروفایل و پست هایتان منتشر میکنید حاوی شماره تلفن، تصویر خانه، مدرسه و یا آدرس تان نباشد.

4 همیشه از اطلاعات مهم مانند عکس ها، فیلم ها، چت ها و فایل های مهم تان نسخه ی پشتیبان و یا Backup بگیرید.

5 برنامه های خود را فقط از منابع معتبر مانند Play Store، App Store، سیب اپ و یا کافه بازار دانلود کنید

شما جایزه ای از بانی مد برنده شدید. برای دریافت جایزه ی خود سایت زیر مراجعه کنید.
Www.banimodjayezebebar.ml

جعلی

برای بردن ۲۰ میلیون تومان در جین وست به سایت زیر مراجعه کنید.
Www.jeanwest۲۰milbebar.iou

جعلی

Figure 40. *Screenshot of the course summary slide.*

6.2 Pre-test and Post-test Development

As mentioned in the previous section, the fourth slide of the session and the last slide are developed to understand how knowledgeable the students see themselves in terms of cybersecurity. Furthermore, the pre-test and post-test are prepared, which can be found in Appendix 4 and 5.

The first two questions of the pre-test are to measure the students' current knowledge of phone security so that it can be compared to the results from post-test. Questions 3 and 4 focus on password security, aiming to understand students' current approaches towards passwords selection. The following two questions record the students' awareness of VPN security, and the last two are to grasp their current practices when receiving an unknown link.

Moreover, Post-test questions follow the same flow as the pre-test. Questions 1 and 2 are to measure whether they recall the information learned in class regarding phone security. Question 3 emphasizes on students' first action when receiving an unknown link. The following two questions are to measure the students' behavioral changes regarding password selection after the training. Finally, the last two questions check whether the students recognize the information learned in training about VPN security.

6.3 Cultural Aspects and Validation of the Developed Course

Upon the end of the course development, the author was requested to run a pre-pilot version of the class for the principal and two other school teachers. The principal requested the pre-pilot on the terms of "due to the class being originated from a Western country, they have to monitor the content before allowing it to be published for the students." During the pre-pilot class, the author was asked to wear Hijab while taking part in an Iranian class. Also, a picture displayed in slide number 2 (which showed a female’s skin) was requested to be changed.

After the pre-pilot training took place and changes were made, the school principal gave the green light to the author to execute the program.

7. ADDIE model Step Four: Implementation

This chapter describes the execution of the pilot class for the proposed cybersecurity awareness program. In order to validate the effectiveness of design, a trial execution is carried out. Due to the time limits and the fact that this research is conducted in Estonia with the focus group located in Iran, the program was executed only one session of 1.5 hours for one of the high school classes in Hormozgan. The schools in Iran are single-sex, and therefore a female class of 27 high school girls aged 17 years old was selected. The school's administrator was contacted, and a guest account was created on the Moodle platform used by the school for the trainer to perform the class. The platform could be accessed using the URL address of https://lms.sultanolama.com/.

Further, the first interactive slide was slide number 4, requesting to rate their knowledge from one to hundred. Meanwhile, the course's last slide was another Wooclap slide, requesting the students to rate their knowledge after the class and name one thing they have learned. A total of 20 responses were received for the pre-knowledge and 26 responses for post-knowledge questions. The results generated are discussed in Chapter 8.

Previous chapter mentioned a test run of the class was organized for the principal and two of the teachers. The comments received from them were addressed, and the final version of the class was produced. The class started by introducing the trainer, and the prepared slides in Chapter 6 were used to convey the training. Upon reaching the slide requesting the students to reply to the question of how to increase phone security, a total of 11 responses were gathered. Half of the responders mentioned setting a solid passcode for phones as the best way to enhance phone security.

Another memorable moment of the class was when the students were asked to guess which of the SMSs shown is real and fake. Regrettably, 48% of the student selected B as the real SMS, whereas the A represents an actual SMS message from the advertising company. The SMSs could be viewed in Figure 39.

Furthermore, when the Password Guessing Game was played in class, a student named Somayeh volunteered. She disclosed information that she was born in 4, Mehr 1383 and 0996 to be the last four digits of her phone number. For more information on converting

Jalali Calendar to Gregorian dates, please refer to [133][134]. The trainer then guessed her password to be Somayeh83, 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*Somayeh*83 or 38!Somayeh!83 or 38@Somayeh@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.

One day before the scheduled class, the pre-test was shared with the school principal, and she distributed it amongst the students, and all 27 responses were gathered. Meanwhile, the post-test was shared after the class, and a total of 23 responses were collected. The number of responses received from both tests are auspicious because it suggests conducting a very comparative evaluation between pre-test and post-test results.

To demonstrate the implementation phase's cultural side, all the requested changes and appearance mentioned in the previous two chapters, such as wearing Hijab for the trainer and the content cleansing, are implemented. Additionally, the structure of online classes is very similar everywhere around the world. Unless infrastructural inadequacies such as access to the Internet or not having a smartphone, online training flow are alike. For this scenario, the class was planned for 29 students; however, two of the students had to relinquish class due to prolonged Internet access.

8. ADDIE model Step Five: Evaluation

Within this chapter, the results of the prototype class carried out are discussed. Despite the fact that only one class was held, the efficacy of the cybersecurity awareness program was assessed using the two criteria. Firstly, distribution of pre-test and post-test amongst the attendees and comparing their gained knowledge; secondly, using the two Wooclap links shared with the students to rank their confidence on cybersecurity concepts before and after the class.

8.1 Pre-test and Post-test Evaluation

We begin with analysing the pre-test and post-test results. Tables 6 and 7 are prepared for more explicit visualization of the evaluation.

Table 6. *Pre-test Results*

No.	Questionnaire item	Options	Value
1	What are the best practices to protect your smartphone and the information stored on it? (you can select more than one)	Have a strong password	24 Votes
		Sharing your passwords with anyone who wants to fix your phone	0 Vote
		Activating find my phone	8 Votes
		Installing applications from anywhere on the web	2 Votes
		Clicking on links which only our friends or family sent us	5 Votes
		Installing antivirus applications	12 Votes
2	In case of an unauthorised access to your phone (for example it being stolen or hacked), what are the best actions to take? (you can select more than one)	Wipe it clean	9 Votes
		Call the police	16 Votes
		I do not care because I do not have anything important on my phone	1 Vote

Continues...

Table 6 – *Continues...*

No	Questionnaire item	Options	Value
		I do not know	10 Votes
3	Which of the following do you use to choose your password?	Combination of my name, birth date and phone number	47.7%
		My national ID number	0.0%
		Contains random combination of letters, digits and symbols	22.2%
		I can remember it but it is difficult to guess	29.6%
		Is the name of the ones I love	0.0%
		Something very easy like 123456 or asdfgh	0.0%
		Something very long and memorable, consisting of 16 characters or more	7.4%
4	My name is Maryam and I want to create an Instagram account for me but I do not know what is the best option to select as my password. I will give you my basic information so that if you can, please help me select a password? ▪ I am 17 years old. I was born in Farvardin, 3rd, 1382 ▪ My phone number is +98 917 123 4567. ▪ My favourite colour is blue ▪ And I love Kabab Please select one option so that I know which one is the best to set my password.	Maryam123	3.7%
		Maryam82	7.4%
		MaryamKabab	7.4%
		Kabab1234	3.7%
		Maryam*123456	3.7%
		123456	11.1%
		P*925DJKdQb	37%
		82Maryam82	25.9%
5	Have you ever thought of possible side effects of using VPNs, for example downloading unwanted malware?	Yes	22.2%
		No	33.3%
		I did not know it has side effects	44.4%

Continues...

Table 6 – *Continues...*

No	Questionnaire item	Options	Value
6	Do you worry about anything when connecting to a VPN?	I do not have any concerns, I just connect to whatever I find online	25.9%
		I do research before connecting to any VPN and find the most secure one to connect	14.8%
		I do not know about the safety myself but I connect to VPNs that are suggested by a professional	59.3%
7	How confident are you that your Hijab-less photos stored on your devices will never get published? Please rate from 1 (less confidence) to 5 (most confidence)	1	3.7%
		2	7.4%
		3	48.1%
		4	25.9%
		5	14.8%
8	Maryam here again. My friend Fatemeh sent me a Whatsapp message with the following content. "BaniMod! To get a 90% off on the spring fashion from us, please visit the following link and enter your home address." If you are interested, you can check the link too.	I clicked on the link because you have sent it	14.8%
		It does not matter who sent it, I will click on it because 90% off is a great deal)	3.7%
		I do not know where the link comes from, I do not click on the link	81.5%
9	Daily we receive many promotional links through SMS, WhatsApp, Telegram, etcetera. They could be from companies advertising or from your friend sharing an interesting content, photo, or video. How do you decide to click on the received link?	Open-ended question. Received answers are discussed below.	

Table 7. *Post-test Results*

No.	Questionnaire item	Options	Value
1	In your opinion, why is it important to secure our phones?	Open-ended question. Received answers are discussed below.	
1	Which of the following is NOT considered an action to increase the phone security?	Activating remote wipes	26.1%
		Calling the police in case of incidents	65.2%
		Installing antivirus applications on your device	4.3%
		Defining a passcode for your device	4.3%
3	We want to help Maryam again. This time, which one is the best option?	Maryam123	0.0%
		Maryam82	4.3%
		MaryamKabab	4.3%
		Kabab1234	0.0%
		Maryam*123456	0.0%
		123456	0.0%
		P*925DJKdQb	82.6%
		82Maryam82	8.7%
4	From now on, which of the following ways do you use to set your passwords?	Combination of my name, birth date and phone number	0.0%
		My national ID number	4.3%
		Contains random combination of letters, digits and symbols	26.1%
		We can remember it but it is difficult to guess	39.1%
		Using the name of the ones we love as passwords	0.0%
		Something very easy like 123456 or asdfgh	0.0%
		Something very long and memorable, consisting of 16 characters or more	30.4%
5	Which of the following is NOT be a disadvantage of using VPN?	Slow Internet	8.7%
		Access to your files	8.7%
		Download unwanted viruses	0.0%
		Change of location	82.6%

Continues...

Table 7 – *Continues...*

No	Questionnaire item	Options	Value
6	When connecting to a VPN for the first time, which of the following should NOT be there?	It allows me to access the filtered applications securely	4.3%
		It accesses my personal files	52.2%
		It changes my location	21.7%
		It secures my Internet traffic	21.7%
7	Imagine you have received this message from your cousin, what are the steps you have to take? To take chance in winning 1 million Toman shopping credit from White Boutique, just click on the bellow link: https://bit.ly/3sKFk0C What is the first thing you must do before clicking on a link that you received from a family member or a friend?	Click	0.0%
		Read	73.9%
		Think	21.7%
		Delete the message	4.3%

The examination of pre-test and post-test questions is performed. Questions 1 and 2 of the pre-test and post-test are designed to analyze students' learning boost on the concept of phone security. During the pre-test, most students selected the correct responses on the best practices to protect smartphones. However, the distress was on ten students who mentioned they do not know what to do when their phones are illegitimately accessed. That is approximately 30% of the total population.

Meanwhile, after the class took place, the students' understanding increased. All of them answered the question of why it is vital to secure phone devices as "because phones contain our personal data such as photos and chats" and "to prevent from being hacked and our personal data manipulated by vigilant people." This shows the increase of their understanding and remembering of what is considered necessary when discussing phone security.

Questions 3 and 4 of pre-test and post-test were aimed at student's knowledge of password security. During pre-test 47.7% of the students selected a combination of their name, birth date, and phone number to describe their current passwords, followed by 29.6% who appointed their passwords to be something they can remember, but it is not easy to guess. When the same question was asked during the post-test examination, the results were considered outstanding as no student mentioned that they will select their name, birth date, and phone number as their passwords from now on. Similarly, two other questions were asked regarding password security in the course of the pre/post-test. During the pre-test, 37% of the students selected "P*925DJKdQb". This number increased to 82% through post-test. 11.1% of responders selected "123456" during the pre-test and this number reached 0% in post-test analysis. In short, the above explanations shows success in meeting the goal of increasing password security awareness and motivating the students to apply the concept in their daily lives.

Questions number 5 and 6 of both pre-test and post-test focuses on VPN security. When students were asked about their knowledge on the possible side effects of using VPNs, more than 44% of the responses indicated that they did not know anything about the side effects, and 33.3% did not bother to care about them. Besides, only 14.8% of the students revealed that they investigate the legitimacy of the VPN before connecting to a VPN. To measure the attendees' understanding, the question of "which of the following could NOT be a disadvantage of using VPN?" was asked during the post-test. 82.6% of the students responded with the correct answer, which was "change of location." This demonstrates that students' knowledge of the side effects of using VPNs increased rapidly. Additionally, more than 50% of the students are warned about non-trusted VPNs' ability to access their personal data. Both of the figures show success in achieving the program goal.

The next item covered in the pre/post-test was student's knowledge and practice in clicking unknown links. Throughout the pre-test period, although only 14.8% of the student mentioned that they would click on the link because a friend had sent the link, when they were asked the open-ended question of how do they decide to click on the received link, 33.3% of them mentioned that depending on the content, they would click on the link. Around 22% mentioned that they would first ask the sender about the link prior to clicking the link. Only one person in the class was persistent in clicking on any link received without any hesitation. The education on the actions to take before clicking a link was completed during the post-test investigation. All of the students, with the exception of one, chose "Read" and "Think" as the first actions to take before clicking on a received link.

To demonstrate a visualization on the comparison of the correct answers received from the students, Tables 8, 9, 10, and 11 are shown. As mentioned earlier, the pre/post-test questions focus on four areas of phone security, password security, VPN security and clicking on unknown links. Because the questions distributed in pre-test and post-test are not the same, and the number of responses received for each test are different, a percentage of the correct answers gathered for each topic is displayed.

Table 8. *Phone Security*

Pre-test question number	**Success responses percentage**	**Post-test question number**	**Success responses percentage**
1	77.7%	1	95.8%
2	62.9%	2	65.2%

Table 9. *Password Security*

Pre-test question number	**Success responses percentage**	**Post-test question number**	**Success responses percentage**
3	39.2%	3	91.3%
4	62.9%	4	95.6%

Table 10. *VPN Security*

Pre-test question number	**Success responses percentage**	**Post-test question number**	**Success responses percentage**
5	22.2%	5	82.6%
6	14.8%	6	52.2%

Table 11. *Clicking on Unknown Links*

Pre-test question number	**Success responses percentage**	**Post-test question number**	**Success responses percentage**
8	81.5%	7	95.6%

8.2 Wooclap Links Evaluation

Subsequently, the results received from the Wooclap links shared at the beginning and end of the class requesting the students to rate their cybersecurity knowledge is analyzed. At the start, the responses were having a mean of 23.27 on the percentage of their current cybersecurity knowledge based on their judgment. However, the average of their knowledge increased at the end of the session. They ranked their knowledge with an average of 58.75, mentioning the following comments:

- I just noticed that I mentioned a wrong percentage at the beginning of the class. The

Internet and cybersecurity are a huge world and what we have learned in this class is a small fraction of it.

- Tips on differentiating fake and real links
- Most of it was new concepts for me
- I moved from 25 percent to 50 percent. Tips on differentiating fake and real links.
- I have learned a lot, like how to select a good password and think before clicking links.
- Introducing trusted VPNs.
- Everything was new to me.
- I recorder a wrong percentage at the beginning. Now I know 30 percent.
- 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 to implement 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.
- I still believe that even if my phone is hacked, there is no harm on me! I do not store anything personal on my phone.
- The course contained very applicable information (4x)

According to the comments received, it can be concluded that the program's aim is achieved, and the students tend to take action and implement the tools shared with them starting from now. Also, it indicates the content prepared for the training was digestible and easy to fetch by the students. During and after the class, none of the students requested more clarification, indicating the clearance of the contents and the message conveying method.

Figure 41 illustrates the relation between the achieved goals of each topic shared in class and their correspondence to Bloom's taxonomy.

To demonstrate the cultural aspects of the Evaluate phase, it is essential to mention that the school principal informed the author on the method used for publishing the pre-test and post-test Google Forms. She identified that the WhatsApp application was used for conveying the documents. This points out the cultural aspect of not using E-mail to communicate in Iran. Although using WhatsApp is an informal way of communication, due to the filtering in Iran and not using E-mail addresses, one of thee main means of communication is the WhatsApp application.

Within this chapter, pre-test and post-test responses, adjacent to the information gathered

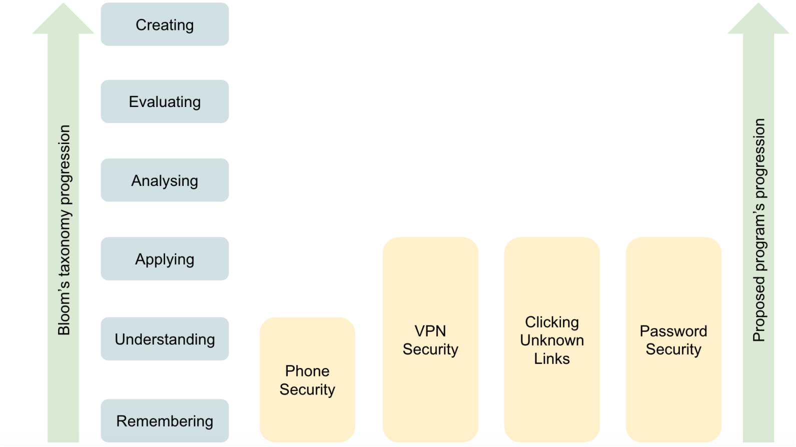


Figure 41. *Proposed course's progression and its correspondence to Bloom's taxonomy.*

on the students' confidence in cybersecurity, were analyzed. Although only one pilot class was implemented, the results were promising. It showed an increase in students' security awareness and motivation to apply and use the tools shared in their daily interaction with the online world.

After the pilot class was run, the author was contacted by two other girl-only high school principals requesting to arrange classes for their school. This was a propitious act as it showed there were more positive feedback forwarded to other principals, and the course was practical.

9. Discussion, Limitations and Future Work

9.1 Discussion

This section emphasizes the ADDIE model's usability with a cultural embrace [1]. This research contributes academically by implementing the ADDIE model with cultural embrace and evaluate its usability and practical aspects of implementation. Even though the model was straightforward and introduced the three I's (Intention, Interaction, and Introspection), it was not as practical as expected. Within the first three stages of the ADDIE model (Analyse, Design, and Develop), the introduction and utilization of the three I's was very advantageous. It provided three different angles when completing the mentioned phases. On the other hand, for the last two stages of the ADDIE model, the three angels were not usable, and they could not be fit in the context of the phases in practice. This suggests that the methodology used could be revised so that the three I's only focus on the Analyse, Design, and Develop stages of the ADDIE model and not on the Implement and Evaluate phases.

Moreover, while the author searched for a Persian cybersecurity training course with a focus on high school students, unfortunately either the courses were too generic or targeting employees [27][28][29][30]. Therefore, it was more convenient to create new training based on the relevant topics found during the survey stage of the research.

Key findings of this research could be summarised in the following items:

- ADDIE model with cultural embrace was not as effective as expected while designing the course
- High school students' cybersecurity knowledge of in Iran, Hormozgan is relatively low
- The course developed should focus on topics listed in Chapter 5
- The pilot class held was successful in increasing students' cybersecurity awareness
- Culture plays an important role in education, and therefore the training content and the process of organizing class are distinct in Iran. More details are discussed in Sections 4.35.56.3.

9.2 Limitations

One limitation was the time to organize the class. The author recognises 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 preliminary pilot's pre/post-test results are indicative for 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 thesis. 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.

9.3 Ethics and Privacy

This research focuses on students who are mainly under 18, meaning they are legally underage. Therefore, it is critical to address the ethical and privacy issues raised by any information exchanged. When preparing the questionnaire and pre/post-test questions, special care was taken to ensure that no personal information was accessed and that the answers were collected anonymously. It is also worth noting that all of the planned material was double-checked with school officials to ensure that it is appropriate for the students. The author contacted the student who revealed her password during the Implementation phase via WhatsApp immediately after class. The student was assisted with how to change her password on various platforms. As a result, no personal information was disclosed during the training.

9.4 Future Work

As mentioned earlier, schools in Iran are single-sex. In the future, it is planned to organize classes for boy-only high schools in Iran. However, there is an additional need to research more on the cultural aspects which could affect boys. So far, all of the mentioned cultural elements could apply to both genders. For example, men in Iran are also considerate to Hijab for the women in their household such as sisters, mothers, and cousins.

Another plan is to run more test cases with both planned classes and gather feedback, so a course titled "Introduction to Cyber Safety and Security" is prepared. Then, the Education

Ministry is contacted so that the course could be added to the high school curriculum. It is believed that the students ought to be aware of the risks of the online world and be motivated to follow the guidelines.

It is planned to post the related course information and upload the slides on virgool.io website so that teachers can access the content [16]. This website is one of the most famous blogging websites in Iran which people tend to post interesting and informative content for public access. There are many educational content uploaded there, such as "How to backup the content of Android phones using Google One" and many more content [135]. Hence, teachers will be better instructed on how to execute and carry out the instruction and be able to download the slides.

10. Summary

It is possible to argue that cyberspace is now more crowded than physical space. Face-to-face experiences are as little as possible due to the global pandemic, so any other daily activity is performed online. Despite the advantages of the virtual world in terms of lifestyle promotion, it has number of disadvantages. Unfortunately, several people, including adolescents, may be unaware of the dangers associated with online activities. As a result, this should serve as an alert to cybersecurity experts, businesses, and schools to raise students' cybersecurity knowledge.

Culture and education, according to Thomas, are inextricably linked in any well-designed program [1]. Thus, one of the attributes of a successful program is its level of engagement with the community it promotes. This research followed the ADDIE instructional design model, using culture as the third dimension [1]. As the focus group for this thesis, the author chose 16 to 18 years old high school students from Iran, Hormozgan Province. The following are the main findings of this research.

1. Despite the fact that no prior research had been conducted on the students' current cybersecurity awareness, the author distributed a questionnaire to gather information on the topic. Based on 616 responses gathered from survey, it was discovered that students do not well understand most basic cybersecurity principles.
2. The author also discovered that several cybersecurity training programs for Iranians had been established, focusing on the business sector and employees. Unfortunately, no initiative targeted students and youth.
3. Because of the differences between the cultures, it was discovered that the Western-developed training courses may not be applicable to Iranian society.
4. The author has indicated that although the ADDIE method with cultural embrace is helpful, the three I's of Intention, Interaction, and Introspection cannot be carried out during the Implement and Evaluate stage of the ADDIE model.
5. The author wrote a section describing the cultural differences between Iran and Western countries in Chapter 2. E-mail usage, Internet censorship and VPNs, and Islamic culture are amongst them.
6. The course content shown elements of uniqueness. For example, the program contains a section on VPN security (which is widely used in Iran) and no section on

E-mail security (which is irrelevant in the Iranian context).

7. Despite the fact that only one pilot class was held, the findings were encouraging, and it was possible to assume that by the end of the course, students' understanding had improved.

To summarize, the study achieved its objectives, and the thesis' goals of raising student awareness and encouraging them to incorporate what they learned in their everyday activities were reached. As a result, potential changes and more trial runs of the class are being planned with the aim of incorporating the course into Iran's high school curriculum.

Bibliography

[1] Michael Thomas, Marlon Mitchell, and Roberto Joseph. “The Third Dimension of ADDIE”. In: *TechTrends* 46.2 ().

[2] *The crime of publishing and threatening to publish private photos and videos*. URL: http://www.heyvalaw.com/web/articles/view/90/%D8%AC%D8%B1%D9%85-%D8%A7%D9%86%D8%AA%D8%B4%D8%A7%D8%B1-%D8%B9%DA%A9%D8%B3-%D9%88-%D9%81%DB%8C%D9%84%D9%85-%D8%AE%D8%B5%D9%88%D8%B5%DB%8C-%D9%88-%D8%AA%D9%87%D8%AF%DB%8C%D8%AF-%D8%A8%D9%87-%D8%A2%D9%86-.html (visited on 03/27/2021).

[3] Serhat Kurt. *Bloom’s Taxonomy - Educational Technology*. 2020. URL: https://educationaltechnology.net/blooms-taxonomy/ (visited on 04/11/2021).

[4] Sonia Livingstone and Ellen Helsper. “Balancing opportunities and risks in teenagers’ use of the internet: The role of online skills and internet self-efficacy”. In: *New media & society* 12.2 (2010), pp. 309–329.

[5] Zainab Hamdan et al. “Protecting teenagers from potential internet security threats”. In: *Proceedings of the 2013 International Conference on Current Trends in Information Technology, CTIT 2013*. IEEE Computer Society, 2013, pp. 143–152. DOI: 10.1109/CTIT.2013.6749493.

[6] Vandra Lea Masemann. “Culture and education”. In: *Comparative education: The dialectic of the global and the local* 2 (2003), pp. 115–132.

[7] . URL: http://www.kashiha.ir/list/daberestan/1th.htm (visited on 02/26/2021).

[8] . URL: http://www.kashiha.ir/list/daberestan/2th.htm (visited on 02/26/2021).

[9] . URL: http://www.kashiha.ir/list/daberestan/3th.htm (visited on 02/26/2021).

[10] Sonia Livingstone and Ellen J Helsper. “Taking risks when communicating on the Internet: The role of offline social-psychological factors in young people’s vulnerability to online risks”. In: *Information, Communication & Society* 10.5 (2007), pp. 619–644.

[11] Eyvind Garder B. Gjertsen et al. “Gamification of Information Security Awareness and Training”. In: *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*. Vol. 1. SCITEPRESS - Science and Technology Publications, 2017, pp. 59–70. ISBN: 978-989-758-209-7. DOI: 10.5220/0006128500590070. URL: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006128500590070.

[12] Arash Parsapour. *Which Social Networking Platforms are used the most amongst Iranian Users?* 2020. URL: https://digiato.com/article/2020/06/29/%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%A7%D9%86-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86%DB%8C-%D8%AF%D8%B1-%DA%A9%D8%AF%D8%A7%D9%85-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D8%AC%D8%AA%D9%85%D8%A7/.

[13] *How many people in Iran use the Internet?* 2017. URL: https://www.tasnimnews.com/fa/news/1396/01/14/1368712/%DA%86%D9%86%D8%AF-%D9%86%D9%81%D8%B1-%D8%AF%D8%B1-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D9%87%D8%B3%D8%AA%D9%86%D8%AF.

[14] Simurgh Aryan, Homa Aryan, and J Alex Halderman. *Internet Censorship in Iran: A First Look*. Tech. rep. 2013. URL: https://www.usenix.org/conference/foci13/workshop-program/presentation/aryan.

[15] Wallace Hannum. “Instructional systems development: A 30 year retrospective”. In: *Educational Technology* 45.4 (2005), pp. 5–21.

[16] *A Place to Write*. URL: https://virgool.io/ (visited on 04/22/2021).

[17] T M Chen and J Robert. “The Evolution of Viruses and Worms”. In: *Statistical methods in computer security* 1 (2004).

[18] Divya R. *CYBER SECURITY FRAMEWORKS FOR THE DIGITAL AGE*. 2019. URL: https://www.dbcollegethal.org/rj/march2019.pdf%7B%5C#%7Dpage=63.

[19] *A Glossary of Common Cyber security Terminology*. 2020. URL: https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary%7B%5C#%7DC.

[20] Rossouw Von Solms and Johan Van Niekerk. "From information security to cyber security". In: *Computers & Security* 38 (2013), pp. 97–102. DOI: 10.1016/j.cose.2013.04.004. URL: http://dx.doi.org/10.1016/j.cose.2013.04.004.

[21] Celia Paulsen and Robert Byers. *Glossary of Key Information Security Terms*. Tech. rep. National Institute of Standards and Technology (NIST), 2019. DOI: https://doi.org/10.6028/NIST.IR.7298r3. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[22] S. S. Tirumala, Abdolhossein Sarrafzadeh, and Paul Pang. "A survey on internet usage and cybersecurity awareness in students". In: *2016 14th Annual Conference on Privacy, Security and Trust, PST 2016*. Institute of Electrical and Electronics Engineers Inc., 2016, pp. 223–228. ISBN: 9781509043798. DOI: 10.1109/PST.2016.7906931.

[23] *Most internet users by country*. URL: https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/.

[24] Behnaz Shoja Heydari. "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*. 1395. URL: https://civilica.com/doc/612746.

[25] Seyed Ali Samouti, Mahmoud Fathy, and Azizipour Mohesen. "A Survey on SAT Cyber Security Awareness Implementation Methods for Managing IT Security". In: *10th International Conference on Information Technology and Knowledge (IKT2019)*. 2019. URL: https://civilica.com/doc/982269.

[26] . 2020. URL: http://csri.majazi.ir/news/90411-%DA%A9%D9%84%D8%A7%D8%B3-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C.html?t=%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1 (visited on 02/26/2021).

[27] Arash Nozari. *Introduction to Cyber Security*. URL: https://cynetco.com/product/intro-to-cyber-security/.

[28] Masoumeh Heydari. *Teaching Cyber Security*. 2020. URL: https://pvlearn.com/product/learn-cyber-security/.

[29] Alireza Ghahrood. *( )*-. 2020. URL: https://evand.com/events/%D8%A8%D9%88%D8%AA-%DA%A9%D9%85%D9%BE-%D8%A7%D8%B1%D8%AA%D9%82%D8%A7%D8%A1-%D8%A2%DA%AF%D8%A7%D9%87%DB%8C-%D8%B1%D8%B3%D8%A7%D9%86%DB%8C-%D8%A7%D9%85%D9%86%

DB%8C%D8%AA-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%AF-76908 (visited on 02/26/2021).

[30] Iranian Cyber Police. –. URL: http://spooler.ir/1395/09/1407/ (visited on 02/28/2021).

[31] *Hormozgan Province*. URL: https://fa.wikipedia.org/wiki/%D8%A7%D8%B3%D8%AA%D8%A7%D9%86%7B%5C_%7D%D9%87%D8%B1%D9%85%D8%B2%DA%AF%D8%A7%D9%86 (visited on 04/11/2021).

[32] Shaykh Baygloo Rana. "SID.ir | IDENTIFYING DEPRIVED REGIONS OF IRAN BY COMPOSITE RANKING". In: *RESEARCH AND URBAN PLANNING* 2.7 (2012), pp. 53–70. URL: https://www.sid.ir/en/journal/ViewPaper.aspx?ID=303388.

[33] Ron Bitton et al. "Taxonomy of mobile users' security awareness". In: *Computers & Security* 73 (2018), pp. 266–293.

[34] Hennie A Kruger and Wayne D Kearney. "A prototype for assessing information security awareness". In: *Computers & security* 25.4 (2006), pp. 289–296.

[35] Mubarak Al-Hadadi and Ali Al Shidhani. "Smartphone security awareness: Time to act". In: *2013 international conference on current trends in information technology (CTIT)*. IEEE. 2013, pp. 166–171.

[36] Iosif Androulidakis and Gorazd Kandus. "A survey on saving personal data in the mobile phone". In: *2011 Sixth International Conference on Availability, Reliability and Security*. IEEE. 2011, pp. 633–638.

[37] Murat Koyuncu and Tolga Pusatli. "Security awareness level of smartphone users: An exploratory case study". In: *Mobile Information Systems* 2019 (2019).

[38] Fayyaadh Parker et al. "Security awareness and adoption of security controls by smartphone users". In: *2015 Second international conference on information security and cyber forensics (InfoSec)*. IEEE. 2015, pp. 99–104.

[39] *Mobile Devices and Security - Networking and Mobile Security | Coursera*. URL: https://www.coursera.org/lecture/security-awareness-training/mobile-devices-and-security-EMjmM?isNewUser=true (visited on 04/11/2021).

[40] *Mobile Security Awareness - Free Online Course*. URL: https://socialmediatraining.com/mobile-security-awareness/ (visited on 04/11/2021).

[41] Aparna Das et al. “Cybersecurity for future presidents: An interdisciplinary non-majors course”. In: *Proceedings of the Conference on Integrating Technology into Computer Science Education, ITiCSE*. New York, NY, USA: Association for Computing Machinery, Mar. 2017, pp. 141–146. ISBN: 9781450346986. DOI: 10.1145/3017680.3017713. URL: https://dl.acm.org/doi/10.1145/3017680.3017713.

[42] Carrie Mccoy and Rebecca Thurmond Fowler. “"You Are the Key to Security": Establishing a Successful Security Awareness Program”. In: *Proceedings of the 32nd annual ACM SIGUCCS conference on User services - SIGUCCS ’04*. New York, New York, USA: ACM Press, 2004. ISBN: 1581138695. URL: http://iatservices.missouri.edu/techknowledge/01-.

[43] Yu Cai and Todd Arney. “Cybersecurity should be taught top-down and case-driven”. In: *SIGITE 2017 - Proceedings of the 18th Annual Conference on Information Technology Education*. Association for Computing Machinery, Inc, Sept. 2017, pp. 103–108. ISBN: 9781450351003. DOI: 10.1145/3125659.3125687. URL: http://dl.acm.org/citation.cfm?doid=3125659.3125687.

[44] David T. Smith and Azad I. Ali. “YOU’VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS”. In: *Issues in Information Systems* 20.1 (2019), pp. 186–194. DOI: https://doi.org/10.48009/1_iis_2019_186-194. URL: https://iacis.org/iis/2019/1%7B%5C_%7Diis%7B%5C_%7D2019%7B%5C_%7D186-194.pdf.

[45] Jack Holdsworth and Edward Apeh. “An effective immersive cyber security awareness learning platform for businesses in the hospitality sector”. In: *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*. IEEE. 2017, pp. 111–117.

[46] D Kaplan. “ways to create a security awareness program people won’t hate”. In: *Retrieved* 12.18 (9), p. 2017.

[47] *Symantec Security Awareness Service*. July 2017. URL: https://docs.broadcom.com/doc/ssap-5-en (visited on 04/11/2021).

[48] Samantha Manke and Ira Winkler. “The habits of highly successful security awareness programs: A cross-company comparison”. In: *Securementem, retrieved April* 12 (2013), p. 2016.

[49] Maria Bada, Angela M Sasse, and Jason R C Nurse. “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?” In: *International Conference on Cyber Security for Sustainable Society* (2015). URL: https://arxiv.org/abs/1901.02672.

[50] Harry C Triandis. “The study of the self has a long tradition in psychology”. In: *Psychological Review* 96.3 (1989), pp. 506–520.

[51] Penelope Lockwood, Tara C. Marshall, and Pamela Sadler. “Promoting success or preventing failure: Cultural differences in motivation by positive and negative role models”. In: *Personality and Social Psychology Bulletin* 31.3 (Mar. 2005), pp. 379–392. ISSN: 01461672. DOI: 10.1177/0146167204271598. URL: http://journals.sagepub.com/doi/10.1177/0146167204271598.

[52] Bilal Khan et al. “Effectiveness of information security awareness methods based on psychological theories”. In: *African Journal of Business Management* 5.26 (2011), pp. 10862–10868. ISSN: 1993-8233. DOI: 10.5897/AJBM11.067. URL: http://www.academicjournals.org/AJBM.

[53] Ira Winkler. *7 elements of a successful security awareness program*. 2017. URL: https://www.csoonline.com/article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html (visited on 11/07/2020).

[54] Mikko T Siponen. “A conceptual foundation for organizational information security awareness”. In: *Information Management & Computer Security* 8.1 (2000), pp. 31–41. URL: https://pdfs.semanticscholar.org/db4e/b7ac502d9cf6cea7e050478c6b018241d54d.pdf.

[55] Jay McTighe and Grant Wiggins. “Understanding by design framework”. In: *Alexandria, VA: Association for Supervision and Curriculum Development* (2012).

[56] John B Biggs and Kevin F Collis. *Evaluating the quality of learning: The SOLO taxonomy (Structure of the Observed Learning Outcome)*. Academic Press, 2014.

[57] Carolyn Fallahi. “Using Fink’s taxonomy in course design”. In: *APS Observer* 24.7 (2011).

[58] *Learning Taxonomies - The Peak Performance Center*. URL: https://thepeakperformancecenter.com/educational-learning/thinking/blooms-taxonomy/learning-taxonomies/ (visited on 04/20/2021).

[59] Patricia Armstrong. “Bloom’s taxonomy”. In: *Vanderbilt University Center for Teaching* (2016).

[60] Mary Forehand. “Bloom’s taxonomy”. In: *Emerging perspectives on learning, teaching, and technology* 41.4 (2010), pp. 47–56.

[61] Jack Conklin. *A taxonomy for learning, teaching, and assessing: A revision of Bloom’s taxonomy of educational objectives complete edition*. 2005.

[62] Marta Orviska and John Hudson. “Dividing or uniting Europe? Internet usage in the EU”. In: *Information Economics and Policy* 21.4 (2009), pp. 279–290.

[63] F. A. Maulana, S. Abdulmana, and F. Alfariti. “Collaborative Internet content filtering on the Internet infrastructure in Malaysia”. In: *2011 International Conference on Uncertainty Reasoning and Knowledge Engineering*. Vol. 1. 2011, pp. 12–15. DOI: 10.1109/URKE.2011.6007822.

[64] Ehsan Shah Ghasemi. “A Revision on the Effects of Virtual Environment on Communication Views”. In: *Global Media Journal* 2 (1385).

[65] Mohammad Mehdi Karimi Zadeh, Ehsan Rafi Zade, and Dariush Kholgh Nik. “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)*. 2015. URL: https://civilica.com/doc/358179.

[66] Helen Spencer-Oatey. “What is culture?” In: (2012).

[67] Helen Spencer-Oatey. “Culturally Speaking Culture, Communication and Politeness Theory 2nd Edition”. In: (2008).

[68] Stephen M Croucher et al. “Religion, culture, and communication”. In: *Oxford Research Encyclopedia of Communication*. 2017.

[69] Max Weber. “The Sociology of Religion, trans”. In: *Ephraim Fischoff (Boston: Beacon, 1963), 00 Notes to* (1963), pp. 290–97.

[70] Jan-Erik Lane and Svante Ersson. “Culture and politics”. In: *A Comparative Approach* 2 (2005).

[71] Ad Chris Garrett. “Developing a security-awareness culture–Improving security decision making”. In: (2004).

[72] Y Al-Shehri and NL Clarke. “Information security awareness and culture”. In: *Advances in Communications, Computing, Networks and Security: Proceedings of the MSc/MRes programmes from the School of Computing, Communications and Electronics, 2007-2008* 6 (2009), p. 12.

[73] Behdad Bakhtiyari and Eghbaleh Azizkhani. “Sociological study of the tendency towards Western values based on the amount and type of use of Internet social networks (Case study of Khalkhal youth)”. In: *Sociological Studies Quarterly* 5.19 (1392), pp. 127–145. URL: https://www.sid.ir/fa/journal/ViewPaper.aspx?ID=263455.

[74] Mohammad Javad Chitsaz and Mohammad Hosseini Moghaddam. “Religiosity and Cyberspace: A Meta-Analysis on the Studies of Religion and Cyberspace”. In: *Journal of Cyberspace Studies* 2.2 (July 2018), pp. 205–228. ISSN: 2588-5502. DOI: 10.22059/JCSS.2018.254328.1015. URL: https://jcss.ut.ac.ir/article%7B%5C_%7D66724.html.

[75] Tabassum F Ruby. “Listening to the voices of hijab”. In: *Women’s Studies International Forum*. Vol. 29. 1. Elsevier. 2006, pp. 54–66.

[76] Sedigheh Karimi. “Iranian Women’s Identity and Cyberspace: Case study of Stealthy Freedom”. In: *Journal of Social Science Studies* 2.1 (Nov. 2014), p. 221. DOI: 10.5296/jsss.v2i1.6284.

[77] *Iran - Wikipedia*. URL: https://en.wikipedia.org/wiki/Iran (visited on 03/27/2021).

[78] Seyed Ali Hoseini and Ali and Ahmadi. “Spatial analysis of the cultural development indicators: Planning Modeling in Hormozgan”. In: *socio-cultural Development Studies* 4.1 (2015). eprint: http://journals.sabz.ac.ir/scds/article-1-273-fa.pdf. URL: http://journals.sabz.ac.ir/scds/article-1-273-fa.html.

[79] *Hacking a young woman’s cell phone at a party caused her a big trouble*. Feb. 2019. URL: https://persianv.com/havades/%D9%85%D8%A7%D8%AC%D8%B1%D8%A7%DB%8C-%D9%87%D9%83-%D9%83%D8%B1%D8%AF%D9%86-%D9%85%D9%88%D8%A8%D8%A7%D9%8A%D9%84.html (visited on 03/27/2021).

[80] Christopher S Leberknight et al. “A taxonomy of Internet censorship and anti-censorship”. In: *Fifth International Conference on Fun with Algorithms*. 2010.

[81] Robert Faris and Nart Villeneuve. “Measuring global Internet filtering”. In: *Access denied: The practice and policy of global Internet filtering* 5 (2008).

[82] *Censorship | Definition of Censorship by Merriam-Webster*. URL: https://www.merriam-webster.com/dictionary/censorship (visited on 03/28/2021).

[83] *Top countries Internet Service Providers (ISP) List*. URL: http://www.ispquicklist.com/TopCountries.aspx (visited on 03/27/2021).

[84] *Iran Internet Service Providers (ISP) List - IspQuickList*. URL: http://www.ispquicklist.com/Internet-Service-Providers-List-in-Iran.aspx (visited on 03/27/2021).

[85] *35% of the most visited sites in the world are blocked in Iran*. Aug. 2019. URL: https://iranintl.com/%D8%AF%D8%A7%D9%86%D8%B4-%D9%88-%D9%81%D9%86%D8%A7%D9%88%D8%B1%DB%8C/%DB%B3%DB%B5-%D8%AF%D8%B1%D8%B5%D8%AF-%D9%BE%D8%B1%D8%A8%D8%A7%D8%B2%D8%AF%DB%8C%D8%AF%D8%AA%D8%B1%DB%8C%D9%86-%D8%B3%D8%A7%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%AC%D9%87%D8%A7%D9%86-%D8%AF%D8%B1-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86-%D9%85%D8%B3%D8%AF%D9%88%D8%AF%D9%86%D8%AF (visited on 03/28/2021).

[86] Muhammad Ikram et al. "An Analysis of the Privacy and Security Risks of Android VPN Permission-Enabled Apps". In: *Proceedings of the 2016 Internet Measurement Conference*. IMC '16. Santa Monica, California, USA: Association for Computing Machinery, 2016, pp. 349–364. ISBN: 9781450345262. DOI: 10.1145/2987443.2987471. URL: https://doi.org/10.1145/2987443.2987471.

[87] *VPN and its Dangers*. URL: http://fampisu.ir/fa/news.php?rid=43 (visited on 04/23/2021).

[88] Vasilis Ververis, Sophia Marguel, and Benjamin Fabian. "Cross-Country Comparison of Internet Censorship: A Literature Review". In: *Policy & Internet* 12.4 (Dec. 2020), pp. 450–473. ISSN: 1944-2866. DOI: 10.1002/poi3.228. URL: https://onlinelibrary.wiley.com/doi/10.1002/poi3.228.

[89] Daniel Baldino and Jarrad Goold. "Iran and the emergence of information and communications technology: the evolution of revolution?" In: *Australian Journal of International Affairs* 68.1 (2014), pp. 17–35.

[90] Magdalena Wojcieszak and Briar Smith. "Will politics be tweeted? New media use by Iranian youth in 2011". In: *New media & society* 16.1 (2014), pp. 91–109.

[91] Martina J Zucule De Barros and Horst Lazarek. "A Cyber Safety Model for Schools in Mozambique". In: *Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal*. 2018, pp. 22–24.

[92] Somayeh Tajik Ismaili and Mojgan Yousef Zadeh. "Investigating the relationship between the amount and type of Internet use and lifestyle". In: *Institute of Humanities and Cultural Studies* 107.2 (1396). URL: http://ensani.ir/fa/article/379744/%D8%A8%D8%B1%D8%B1%D8%B3%DB%8C-%D8%B1%D8%A7%D8%A8%D8%B7%D9%87-%D9%85%DB%8C%D8%A7%D9%86-%D9%85%DB%8C%D8%B2%D8%A7%D9%86-%D9%88-%D9%86%D9%88%D8%B9-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D8%A7%D8%B2-%D8%A7%DB%8C%D9%86%D8%AA%

D8%B1%D9%86%D8%AA-%D8%A8%D8%A7-%D8%B3%D8%A8%DA%A9-%D8%B2%D9%86%D8%AF%DA%AF%DB%8C.

[93] *bama*. URL: https://bama.ir/ (visited on 04/09/2021).

[94] *::: Iran-Tejarat.com :::* URL: http://iran-tejarat.com/Register/Register.html (visited on 04/09/2021).

[95] Letha H. Etzkorn, Carl G. Davis, and Lisa L. Bowen. “The language of comments in computer software: A sublanguage of English”. In: *Journal of Pragmatics* 33.11 (2001), pp. 1731–1756. ISSN: 0378-2166. DOI: https://doi.org/10.1016/S0378-2166(00)00068-0. URL: https://www.sciencedirect.com/science/article/pii/S0378216600000680.

[96] Ahrari Ghafoor and Habibi Jamileh. “Media literacy, English language and lifelong learning triangle thinking skills”. In: *National Conference on Primary Education*. 1394. URL: https://www.sid.ir/fa/seminar/ViewPaper.aspx?ID=58732.

[97] F Zarrabi and JR Brown. “English language teaching and learning analysis in Iran”. In: *International Journal of Educational and Pedagogical Sciences* 9.10 (2017), pp. 3485–3493.

[98] Yaser Khajavi and Reza Abbasian. “English language in Iran: Why practice is more common than practise?” In: *Canadian Social Science* 7.4 (2011), pp. 89–94.

[99] *Free WiFi Hotspots in Tehran | WiFi Map*. URL: https://www.wifimap.io/1571-tehran-free-wifi (visited on 04/10/2021).

[100] Amir Mastkin and Amin Ghiasi. *Free Public Internet; Reality or a Dream?* URL: https://digiato.com/article/2017/10/28/%D8%A7%D8%B1%D8%A7%D8%A6%D9%87-wifi-%D8%B9%D9%85%D9%88%D9%85%DB%8C-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D8%B1-%D8%A7%DB%8C%D8%B1%D8%A7%D9%86/ (visited on 04/10/2021).

[101] *What is a Cookie? How it works and ways to stay safe | Kaspersky*. URL: https://www.kaspersky.com/resource-center/definitions/cookies (visited on 04/10/2021).

[102] Vahid Tahmasebi. *What Are the Best Iranian Sites*. URL: https://karsazsho.com/what-are-the-best-iranian-sites/ (visited on 04/10/2021).

[103] Robert M Gagne et al. *Principles of instructional design*. 2005.

[104] M David Merrill. “First principles of instruction”. In: *Educational technology research and development* 50.3 (2002), pp. 43–59.

[105] *Instructional Design Models: Comparing ADDIE, Bloom, Gagne, Merrill.* URL: https://www.dashe.com/blog/instructional-design-models-comparing-addie-bloom-gagne-merrill (visited on 04/20/2021).

[106] G Muruganantham. “Developing of E-content package by using ADDIE model”. In: *International Journal of Applied Research* 1.3 (2015), pp. 52–54.

[107] Sharon A Shrock. “A brief history of instructional development”. In: *Instructional technology: Past, present, and future* 2 (1995), pp. 11–19.

[108] Leslie J Briggs. *Instructional design: Principles and applications*. Educational Technology, 1991.

[109] William R Tracey, Edward B Flynn Jr, and CL Legere. *The development of instructional systems*. Tech. rep. ARMY SECURITY AGENCY TRAINING CENTER and SCHOOL FORT DEVENS MA, 1970.

[110] Donn C Ritchie and Bob Hoffman. “Using instructional design principles to amplify learning on the World Wide Web”. In: *Society for Information Technology & Teacher Education International Conference*. Association for the Advancement of Computing in Education (AACE). 1996, pp. 845–847.

[111] Michael Molenda. “In search of the elusive ADDIE model”. In: *Performance improvement* 42.5 (2003), pp. 34–37.

[112] Steven J Bell and John D Shank. *Academic librarianship by design: A blended librarian’s guide to the tools and techniques*. American Library Association, 2007.

[113] Paul Clayton Campbell. “Modifying ADDIE: Incorporating new technologies in library instruction”. In: *Public Services Quarterly* 10.2 (2014), pp. 138–149.

[114] Tzu-Chuan Hsu et al. “Using the ADDIE model to develop online continuing education courses on caring for nurses in Taiwan”. In: *The Journal of Continuing Education in Nursing* 45.3 (2014), p. 124.

[115] Angiah L Davis. “Using instructional design principles to develop effective information literacy instruction: The ADDIE model”. In: *College & Research Libraries News* 74.4 (2013), pp. 205–207.

[116] AW Tony Bates et al. “4.3 The ADDIE model”. In: *Teaching in a Digital Age* (2015).

[117] Elspeth McKay et al. “Prescriptive training courseware: IS-design methodology”. In: *Australasian Journal of Information Systems* 22 (2018).

[118] Serhat Kurt. *ADDIE Model: Instructional Design*. 2017. URL: https://educationaltechnology.net/the-addie-model-instructional-design/ (visited on 04/13/2021).

[119] John Biggs. “The reflective institution: Assuring and enhancing the quality of teaching and learning”. In: *Higher education* 41.3 (2001), pp. 221–238.

[120] Talal Alodwan and Mosaab Almosa. “The Effect of a Computer Program Based on Analysis, Design, Development, Implementation and Evaluation (ADDIE) in Improving Ninth Graders’ Listening and Reading Comprehension Skills in English in Jordan.” In: *English Language Teaching* 11.4 (2018), pp. 43–51.

[121] *World Data Atlas - Iran, Hormozgan*. URL: https://knoema.com/atlas/Iran/Hormozgan.

[122] Robin Hill. “What sample size is “enough” in internet survey research”. In: *Interpersonal Computing and Technology: An electronic journal for the 21st century* 6.3-4 (1998), pp. 1–12.

[123] Eben. *How important are teaching methods (approaches) for ideal results in education?. A WHATSAPP deliberation on CME*. 2018. URL: http://creativemindeduco.com/how-important-are-teaching-methods-approaches-for-ideal-results-in-education-a-whatsapp-deliberation-on-cme/ (visited on 02/18/2021).

[124] *Domestic platform for webinars, web conferences and online training - Skyroom*. URL: https://www.skyroom.online/%7B%5C#%7Duse-cases (visited on 04/12/2021).

[125] David R Krathwohl. “Theory Into Practice A Revision of Bloom’s Taxonomy: An Overview”. In: *Theory Into Practice* 41.4 (2010), pp. 212–218. ISSN: 1543-0421. DOI: 10.1207/s15430421tip4104_2. URL: https://www.tandfonline.com/action/journalInformation?journalCode=htip20.

[126] Pearl Jacobs. “The challenges of online courses for the instructor”. In: (2013). URL: https://digitalcommons.sacredheart.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1007&context=cj_fac.

[127] *Wooclap - An interactive platform that makes learning awesome*. URL: https://www.wooclap.com/ (visited on 04/02/2021).

[128] Beryl Blaustone. “Teaching Evidence: Storytelling in the Classroom”. In: *American University Law Review* 41 (1991). URL: https://heinonline.org/HOL/Page?handle=hein.journals/aulr41%7B%5C&%7Did=494%7B%5C&%7Ddiv=18%7B%5C&%7Dcollection=journals.

[129] Angela Felix. “Using pre/post-testing to evaluate the effectiveness of online language programs”. In: *Journal of Second Language Teaching & Research* 4.1 (2016), pp. 176–193.

[130] *Communication development projects and access to the Internet in some villages of Hormozgan were inaugurated - Bazaar News Agency - Bazaar news site*. URL: https://www.tahlilbazaar.com/news/78503/%D9%BE%D8%B1%D9%88%DA%98%D9%87-%D9%87%D8%A7%DB%8C-%D8%AA%D9%88%D8%B3%D8%B9%D9%87-%D8%A7%D8%B1%D8%AA%D8%A8%D8%A7%D8%B7%D8%A7%D8%AA-%D9%88-%D8%AF%D8%B3%D8%AA%D8%B1%D8%B3%DB%8C-%D8%A8%D8%B1%D8%AE%DB%8C-%D8%A7%D8%B2-%D8%B1%D9%88%D8%B3%D8%AA%D8%A7%D9%87%D8%A7%DB%8C-%D9%87%D8%B1%D9%85%D8%B2%DA%AF%D8%A7%D9%86-%D8%A8%D9%87 (visited on 04/12/2021).

[131] *Destruction of the young lady's life through her hacked phone*. URL: https://persianv.com/havades/%D9%85%D8%A7%D8%AC%D8%B1%D8%A7%DB%8C-%D9%87%D9%83-%D9%83%D8%B1%D8%AF%D9%86-%D9%85%D9%88%D8%A8%D8%A7%D9%8A%D9%84.html (visited on 04/02/2021).

[132] *Google Safe Browsing – Google Transparency Report*. URL: https://transparencyreport.google.com/safe-browsing/overview (visited on 04/02/2021).

[133] *Iranian calendars - Wikipedia*. URL: https://en.wikipedia.org/wiki/Iranian%7B%5C_%7Dcalendars (visited on 04/02/2021).

[134] *Iranian Calendar - HoomanB.com*. URL: http://www.hoomanb.com/calendar/jalali%7B%5C_%7Dcalendar.php?jyear=1383%7B%5C&%7Djmonth=7%7B%5C&%7Djday=4 (visited on 04/02/2021).

[135] *Learn how to back up your Android phone with Google One - Virgool*. URL: https://virgool.io/@digipars/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%A8%DA%A9%D8%A7%D9%BE-%DA%AF%D8%B1%D9%81%D8%AA%D9%86-%D8%A7%D8%B2-%DA%AF%D9%88%D8%B4%DB%8C-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF-%D8%A8%D8%A7-%DA%AF%D9%88%DA%AF%D9%84-%D9%88%D8%A7%D9%86-i3iekekuyja1 (visited on 04/22/2021).

Appendices

Appendix 1 - Questionnaire in English

How old are you?
a) 13-15
b) 16-18
c) Other (please specify)

What is your gender?
a) Male
b) Female

What type of devices do you use to connect to the internet?
a) Only smartphone
b) Only laptop
c) Only Tablet
d) Using Smartphone, Tablet, or Laptop

How often do you use the Internet (it includes using Whatsapp, Instagram, Telegram, etc)?
a) Less than 2 hours per day
b) 2 to 5 hours per day
c) 5 to 10 hours per day
d) 10 to 12 hours per day
e) I am constantly on my phone except the time I am sleeping

Which is your most used app on your phone?(You can select more than one) WhatsApp
a) Instagram
b) Telegram
c) Gmail/Yahoo Mail
d) Facebook
e) Snapchat

f) Others (please specify)

Do you click on links you receive on Whatsapp or Telegram?
a) Yes, always and without hesitation
b) Sometimes, if the caption of the message is interesting or it is from someone I trust
c) Never, I do not click on the links that I don’t recognise

Do you have any backup for your chats, photos, etc ?
a) Yes, I constantly backup my data Sometimes, I have a backup of my data from few weeks or months back
b) No, I do not have anything important
c) No, I do not know how to backup my data

When do you switch on VPN?
a) It is always on, I rarely switch it off Only when I am using specific applications
b) I never use any VPNs
c) I do not know what a VPN is

In case you are using VPN for specific applications, please specify them here.

Do you purchase your VPN?
a) Yes, I do purchase them.
b) No, I use free versions of different applications.
c) No, I do not use VPN or I do not know what VPN is.

Do you know anything about VPN security?
a) Yes, I completely know what it is
b) To some extent, I have read about it
c) No, I have never heard of it

Please explain in few sentences your knowledge on VPN security

Do you know what password security is?
a) Yes, I completely know what it is
b) To some extent, I have read about it
c) No, I have never heard of it

In your opinion, what makes a password strong?
a) A combination of random numbers, letters and characters

b) A combination of your name with some number
c) Your name, birthdate and phone number
d) A very easy name or number to remember

Please explain in a few sentences how to choose a strong password.

Have you ever discussed your password to one of your accounts, email, instagram, telegram, etc over social networks (example Instagram) or in person with someone else?
a) Always, I have nothing to hide.
b) Yes, when it is necessary either through public or private channels.
c) Only for emergencies and in private chat, never through a public channel.
d) Never, password is personal information.
e) I do not use passwords

Have you ever asked a family member or a friend to help you fix an issue in one of your online accounts and shared the password with him/her?
a) Yes, I asked for help but did not share my password
b) Yes, I asked for help and shared my password with them
c) Never, I always solved my problems by myself

If yes, did you change your password later on?
a) No, I do not think it is necessary, I trust that person
b) No, I do not know how to change the password.
c) Yes, I always change the password.

In your opinion, is it possible that someone abuses your phone or laptop device which is left unattended while it is logged in?
a) No, because I do not have anything confidential on my devices.
b) No, because no one cares about my devices.
c) Yes, people can take advantage of my logged in social media account
d) Yes, it is very highly possible that my devices are used to send fake messages and my phone number is abused.

Are you familiar with phone antivirus applications?
a) Yes, I always have it installed on my phone
b) Yes, I know what it is but I do not have it installed in my phone because I do not think it is important
c) No, I do not know what it is
d) I do not know if it is installed or not

Are you familiar with the software, operating system and application updates request on your phone or computer?

a) Yes, I know what they are and I activated the automatic update so they get updated once the new versions are out

b) Yes, I know what they are and I see them and I immediately install the updates manually.

c) Yes, I know what they are and but I delay the updates as much as I can until they force update the applications

d) Yes, I know what they are but I do not care about updating and I do not like the waiting time, so I never update my applications

e) No, I do not know what the software, operating system and application updates means

Have you ever heard of phishing attacks?

a) Yes, I have read about it

b) Yes, I have been a victim of a phishing attack

c) No, I have never heard of them

Can you tell me what a phishing attack is? You can explain with an example.

Have you ever been a victim of a cyber attack?

a) Yes

b) No

In case you have been a cyber attack victim, can you please explain the event?

Have you ever been hacked?

a) Yes, I have been hacked before

b) No, but I know someone who has been hacked before

c) No, neither me or anyone that I know has been hacked before

d) No, I do not know what hacking is

Are you familiar with the concept of cyberbullying?

a) Yes, I have read about it but never been cyberbullied

b) Yes, I have been cyberbullied before

c) Yes, I know someone who has been cyberbullied before

d) No, I do not know what cyberbullying is

Have you even received any negative words/comments/messages through WhatsApp/Telegram/Instagram? (examples are: “you are fat”, “you are ugly”, “you are stupid”, etc)

a) Yes

b) No

Have you ever received a cyber security awareness training?
a) Yes
b) No

In case you have taken the cyber security awareness classes before, please specify their negative and positive impacts as well as the topics discussed.

What is your preferred learning method? (You can select more than one)
a) Lectures
b) Seminars/webinars
c) Group work
d) Through videos
e) Through PowerPoint slides
f) Using some practical exercises through website

Appendix 2 - Principal Interview Questions and Responses

Question:
What are the challenges you face when organizing classes online?
Answer:

- Classes getting cancelled because many of the students are not able to join due to low internet speed
- Students not attending classes due to slow internet
- Students not replying due to the improper condition at home or technical issues with their devices
- The quality of the content reduces even though the teachers spend more time to prepare it. This is because the teachers cannot control the students or interact with them
- Students are discouraged due to the lack of interaction between the students and teachers

Question:
In your opinion, what is the most suitable platform for executing the training?
Answer:
Using the Moodle platform. It is good because:

- It does not need to be downloaded
- It contains useful tools such as a whiteboard
- Ability to upload files
- Streaming online class

Question:
What is the current teaching culture?
Answer:
Unfortunately, currently the content of many courses does not prepare students for application of materials learned. So mostly students just forget about everything and not implement them in real life after their exams.

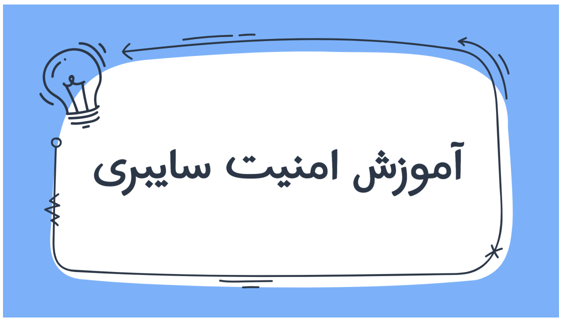
Online:

- Using Moodle (BigBlueButton) to organize classes
- Recording a voice message or a video clip explaining the class and sharing with the students through WhatsApp
- Uploading educational videos found online on the Moodle platform
- For exams, video calls take place over WhatsApp applications so that the teachers can ask students the questions in mind.
- Another method is called reverse-learning, in which teachers ask the students to go through specific chapters of the book and contact the teacher if they have any questions or need more clarifications.

Face-to-face classes:
When in class, the majority of classes are organized traditionally, the way that the teachers explain the concepts and students are to memorise. Some classes like Mathematics, students might be asked to come to the board and solve a problem. But humanitarian or other courses follow the traditional teacher-oriented teaching method.

Question:
What applications are used for conveying information?
Answer:
WhatsApp application and the Moodle platform

Appendix 3 - Teaching slides



آموزش امنیت سایبری

Figure 42. Screenshot of the introductory slide

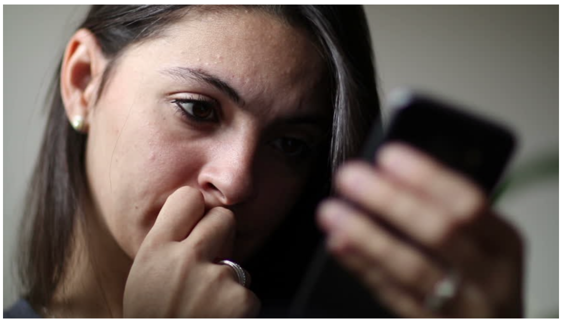
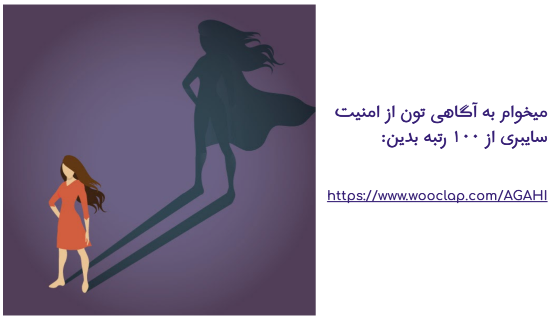


Figure 43. Screenshot of the starting story slide

سایبر سکیوریتی چیست؟

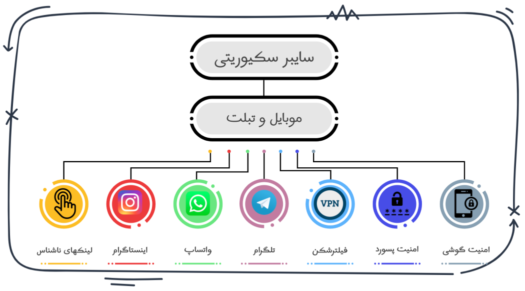
Figure 44. Screenshot of the cybersecurity definition slide



میخوام به آگاهی تون از امنیت سایبری از ۱۰۰ رتبه بدین:

https://www.wooclap.com/AGAHI

Figure 45. Screenshot of the slide asking for the rate of initial knowledge of the students



سایبر سکیوریتی

موبایل و تبلت

امنیت گوشی

امنیت پسورد

فیلترشکن

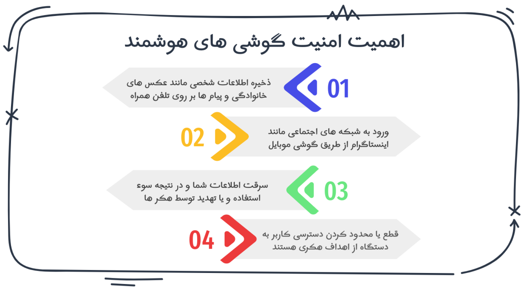
تلگرام

واتساپ

اینستاگرام

لینکهای ناشناس

Figure 46. Screenshot of the course content slide



اهمیت امنیت گوشی های هوشمند

01 ذخیره اطلاعات شخصی مانند عکس های خانوادگی و پیام ها بر روی تلفن همراه

02 ورود به شبکه های اجتماعی مانند اینستاگرام از طریق گوشی موبایل

03 سرقت اطلاعات شما و در نتیجه سوء استفاده و یا تهدید توسط هکر ها

04 قطع یا محدود کردن دسترسی کاربر به دستگاه از اهداف هکری هستند

Figure 47. Screenshot of the slide on the importance of phone security

برای بالا بردن امنیت گوشی، چه کارهایی میتوانیم انجام دهیم؟

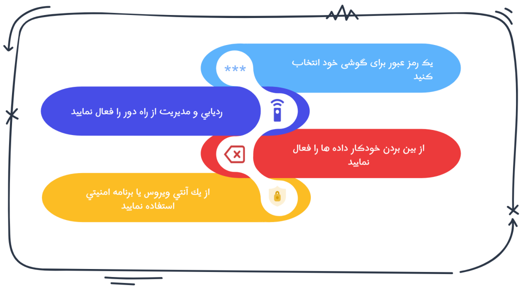
https://www.wooclap.com/GOOSHI

Figure 48. Screenshot of the slide requesting for a volunteer on how to increase phone security

برای بالا بردن امنیت گوشی، چه کارهایی میتوانیم انجام دهیم؟

کسی داوطلب میشه بهم بگه؟

Figure 49. Screenshot of the slide containing Wooclap link on how to increase phone security



یک رمز عبور برای گوشی خود انتخاب کنید

ردیابي و مدیریت از راه دور را فعال نمایید

از بین بردن خودکار داده ها را فعال نمایید

از يك آنتي ویروس یا برنامه امنيتي استفاده نمایید

Figure 50. Screenshot of the slide illustrating guidelines for increasing phone security

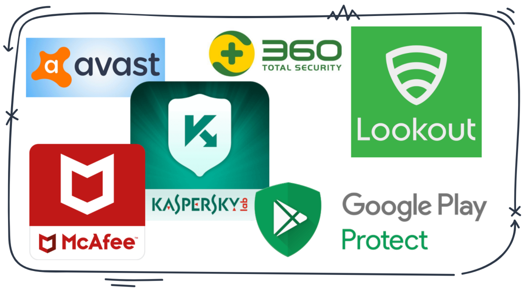
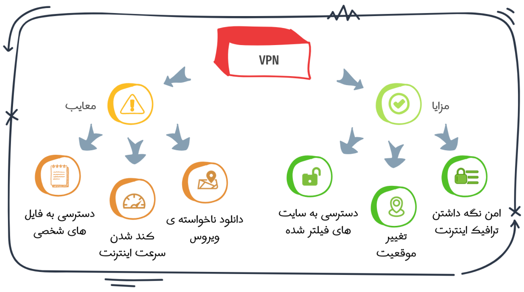


Figure 51. Screenshot of the slide demonstrating trusted antiviruses

VPN چیست

Figure 52. Screenshot of the VPN definition slide



VPN

معایب

دسترسی به فایل های شخصی

کند شدن سرعت اینترنت

دانلود ناخواسته ی ویروس

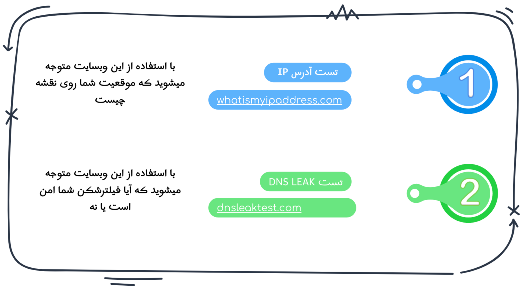
مزایا

دسترسی به سایت های فیلتر شده

تغییر موقعیت

امن نگه داشتن ترافیک اینترنت

Figure 53. Screenshot of the slide containing advantages and disadvantages of VPNs



1 تست آدرس IP

whatismyipaddress.com

با استفاده از این وبسایت متوجه میشوید که موقعیت شما روی نقشه چیست

2 تست DNS LEAK

dnsleaktest.com

با استفاده از این وبسایت متوجه میشوید که آیا فیلترشکن شما امن است یا نه

Figure 54. Screenshot of the slide illustrating two helpful links to indicate the security of VPN

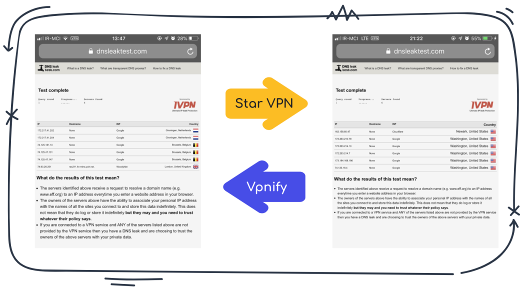


Figure 55. Screenshot of the slide showing results of two example VPNs DNSleak website

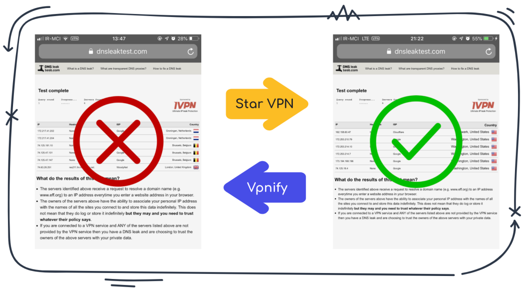


Figure 56. Screenshot of the slide demonstrating secure and insecure VPNs

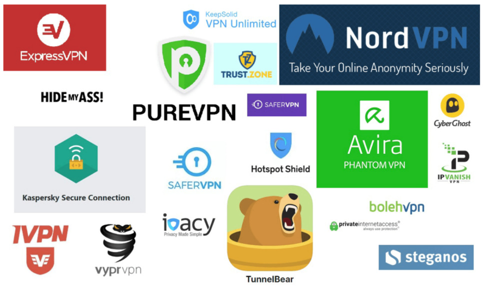


Figure 57. Screenshot of the slide demonstrating trusted VPNs

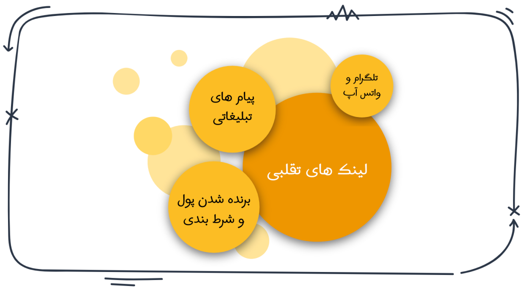
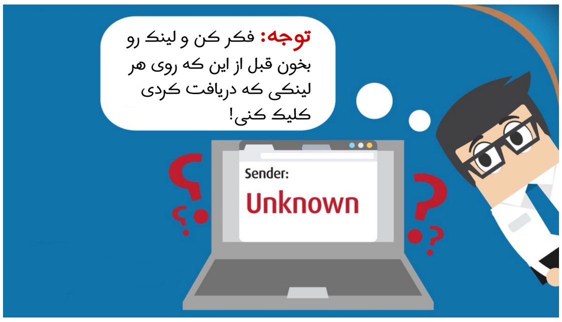


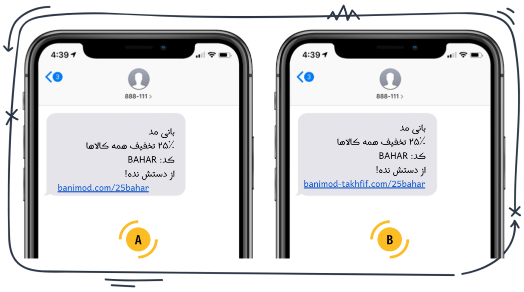
Figure 58. Screenshot of the slide indicating ways we receive links



توجه: فکر کن و لینک رو
بخون قبل از این که روی هر
لینکی که دریافت کردی
کلیک کنی!

Sender:
Unknown

Figure 59. Screenshot of the slide containing a message to read before click



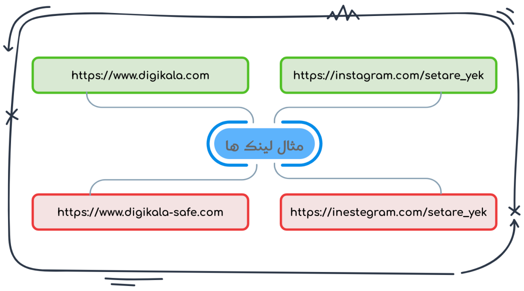
4:39
888-111
بانی مد
۲۵٪ تخفیف همه کالاها
کد: BAHAR
از دستش نده!
banimod.com/25bahar

A

4:39
888-111
بانی مد
۲۵٪ تخفیف همه کالاها
کد: BAHAR
از دستش نده!
banimod-takhfif.com/25bahar

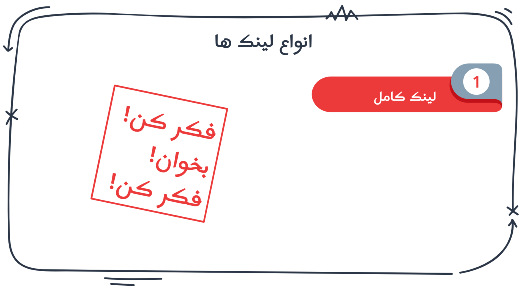
B

Figure 60. Screenshot of two SMSs received, and students are required to identify the real SMS



https://www.digikala.com
https://instagram.com/setare_yek
مثال لینک ها
https://www.digikala-safe.com
https://inestegram.com/setare_yek

Figure 61. Screenshot of two examples of fake and legitimate URLs slide

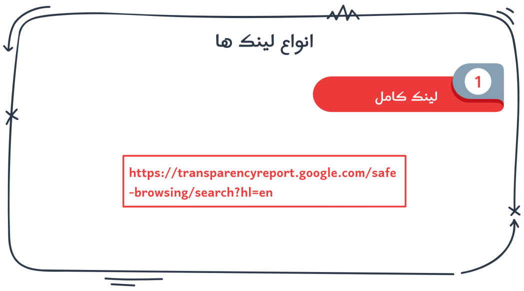


انواع لینک ها

1 لینک کامل

فکر کن!
بخوان!
فکر کن!

Figure 62. Screenshot of the slide representing the long URL and read before click

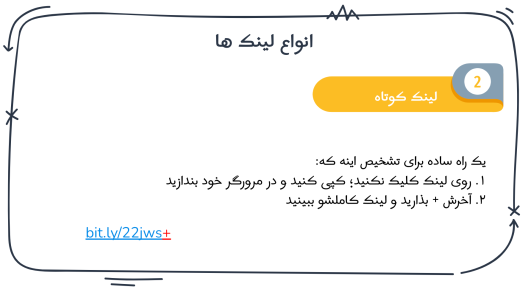


انواع لینک ها

1 لینک کامل

https://transparencyreport.google.com/safe-browsing/search?hl=en

Figure 63. Screenshot of the slide introducing Google Transparency Report



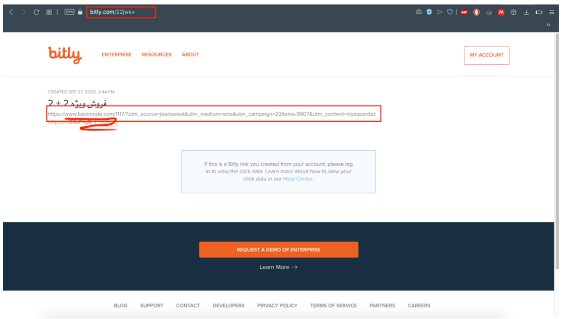
انواع لینک ها

2 لینک کوتاه

یک راه ساده برای تشخیص اینه که:
۱. روی لینک کلیک نکنید؛ کپی کنید و در مرورگر خود بندازید
۲. آخرش + بذارید و لینک کاملشو ببینید

bit.ly/22jws+

Figure 64. Screenshot of the slide representing the short URL and how to check bitly URLs



bitly.com/22jws+

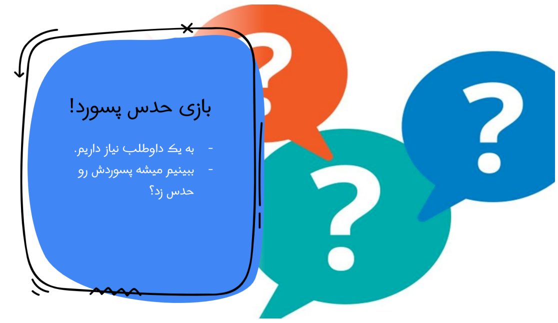
CREATED SEP 27, 2020, 2:44 PM

فروش ویژه 2 + 2

https://www.banimode.com/1117/?utm_source=jeanswest&utm_medium=sms&utm_campaign=22items-9907&utm_content=niyazpardaz

If this is a Bitly link you created from your account, please log in to view the click data. Learn more about how to view your click data in our Help Center.

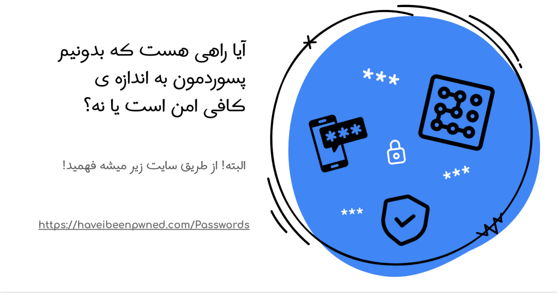
Figure 65. Screenshot of the slide portraying example of a short URL checked



بازی حدس پسورد!

- به یک داوطلب نیاز داریم.
- ببینیم میشه پسوردش رو حدس زد؟

Figure 66. Screenshot of the slide introducing the Password Guessing Game

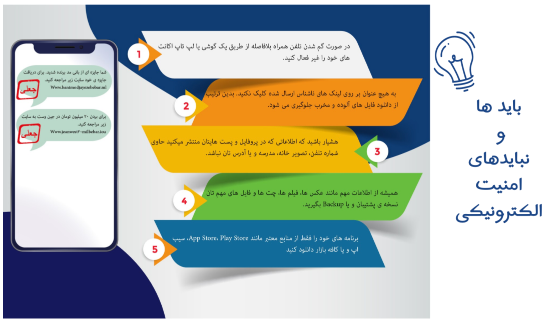


آیا راهی هست که بدونیم
پسوردمون به اندازه ی
کافی امن است یا نه؟

البته! از طریق سایت زیر میشه فهمید!

https://haveibeenpwned.com/Passwords

Figure 67. Screenshot of the slide suggesting the use of haveibeenpwned website



شما جایزه ای از بانی مد برنده شدید. برای دریافت جایزه ی خود سایت زیر مراجعه کنید.
Www.banimodjayezebebar.ml
جعلی

برای بردن ۲۰ میلیون تومان در جین وست به سایت زیر مراجعه کنید.
Www.jeanwest۲۰milbebar.iou
جعلی

1 در صورت گم شدن تلفن همراه بلافاصله از طریق یک گوشی یا لپ تاپ اکانت های خود را غیر فعال کنید.

2 به هیچ عنوان بر روی لینک های ناشناس ارسال شده کلیک نکنید. بدین ترتیب از دانلود فایل های آلوده و مخرب جلوگیری می شود.

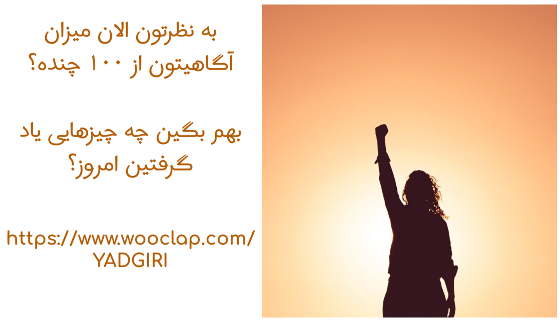
3 هشیار باشید که اطلاعاتی که در پروفایل و پست هایتان منتشر میکنید حاوی شماره تلفن، تصویر خانه، مدرسه و یا آدرس تان نباشد.

4 همیشه از اطلاعات مهم مانند عکس ها، فیلم ها، چت ها و فایل های مهم تان نسخه ی پشتیبان و یا Backup بگیرید.

5 برنامه های خود را فقط از منابع معتبر مانند Play Store، App Store، سیب اپ و یا کافه بازار دانلود کنید

باید ها
و
نبایدهای
امنیت
الکترونیکی

Figure 68. Screenshot of the course summary slide



به نظرتون الان میزان
آگاهیتون از ۱۰۰ چنده؟

بهم بگین چه چیزهایی یاد
گرفتین امروز؟

https://www.wooclap.com/
YADGIRI

Figure 69. Screenshot of the slide asking the students to their final knowledge

Appendix 4 - Pre-test Questions

What are the best practices to protect your smartphone and the information stored on it? (you can select more than one)
a) Have a strong password
b) Sharing your passwords with anyone who wants to fix your phone
c) Activating find my phone
d) Installing applications from anywhere on the web
e) Clicking on links which only our friends or family sent us
f) Installing antivirus applications

In case of an unauthorised access to your phone (for example it being stolen or hacked), what are the best actions to take? (you can select more than one)
a) Wipe it clean
b) Call the police
c) I do not care because I do not have anything important on my phone
d) I do not know

Which of the following do you use to choose your password?
a) Combination of my name, birth date and phone number
b) My national ID number
c) Contains random combination of letters, digits and symbols
d) I can remember it but it is difficult to guess
e) Is the name of the ones I love
f) Something very easy like 123456 or asdfgh
g) Something very long and memorable, consisting of 16 characters or more

My name is Maryam and I want to create an Instagram account for me but I do not know what is the best option to select as my password. I will give you my basic information so that if you can, please help me select a password?
I am 17 years old. I was born in 3 Farvardin, 1382
My phone number is +98 917 123 4567.
My favourite colour is blue
And I love Kabab

Please select one option so that I know which one is the best to set my password.
a) Maryam123
b) Maryam82
c) MaryamKabab
d) Kabab1234
e) Maryam*123456
f) 123456
g) P*925DJKdQb
h) 82Maryam82

Have you ever thought of possible side effects of using VPNs, for example downloading unwanted malware?
a) Yes
b) No
c) I did not know it has side effects

Do you worry about anything when connecting to a VPN?
a) I do not have any concerns, I just connect to whatever I find online.
b) I do research before connecting to any VPN and find the most secure one to connect.
c) I do not know about the safety myself but I connect to VPNs that are suggested by a professional.

How confident are you that your Hijab-less photos stored on your devices will never get published? Please rate from 1 (less confidence) to 5 (most confidence)
a) 1
b) 2
c) 3
d) 4
e) 5

Maryam here again. My friend Fatemeh sent me a Whatsapp message with the following content.
"BaniMod! To get a 90% off on the spring fashion from us, please visit the following link and enter your home address." If you are interested, you can check the link too.
a) I clicked on the link because you have sent it
b) It does not matter who sent it, I will click on it because 90% off is a great deal)
c) I do not know where the link comes from, I do not click on the link

Daily we receive many promotional links through SMS, WhatsApp, Telegram, etcetera.

They could be from companies advertising or from your friend sharing an interesting content, photo, or video. How do you decide to click on the received link? Open-ended question. Received answers are discussed below.

Appendix 5 - Post-test Questions

In your opinion, why is it important to secure our phones?

Which of the following is NOT considered an action to increase the phone security?
a) Activating remote wipes
b) Calling the police in case of incidents
c) Installing antivirus applications on your device
d) Defining a passcode for your device

We want to help Maryam again. This time, which one is the best option?
a) Maryam123
b) Maryam82
c) MaryamKabab
d) Kabab1234
e) Maryam*123456
f) 123456
g) P*925DJKdQb
h) 82Maryam82

From now on, which of the following ways do you use to set your passwords?
a) Combination of my name, birth date and phone number
b) My national ID number
c) Contains random combination of letters, digits and symbols
d) I can remember it but it is difficult to guess
e) Is the name of the ones I love
f) Something very easy like 123456 or asdfgh
g) Something very long and memorable, consisting of 16 characters or more

Which of the following is NOT be a disadvantage of using VPN?
a) Slow internet
b) Access to your files
c) Download unwanted viruses
d) Change of location

When connecting to a VPN for the first time, which of the following should NOT be there?
a) It allows me to access the filtered applications securely
b) It accesses my personal files
c) It changes my location
d) It secures my internet traffic

Imagine you have received this message from your cousin, what are the steps you have to take?
To take chance in winning 1 million Toman shopping credit from White Boutique, just click on the bellow link:
https://bit.ly/3sKFk0C
What is the first thing you must do before clicking on a link that you received from a family member or a friend?
a) Click
b) Read
c) Think
d) Delete the message