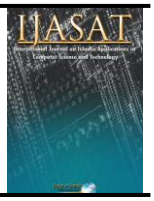

Awareness Level of the Cyber Security and Ethics at Students in University of Ha'il

Lamya Khalid Alsumair [1], Meiad Jrad Aljrad [2], Nujud Ahmed Alghurairy [3], Hind Khalid Alswayegh [4], Modhi Alanazi [5], Kawther Al-Dhlan

[1,2,3,4,5] Cybersecurity, College of Computer Science and Engineering, University of Hail, Kingdom of Saudi Arabia
[1] Lamya2012_@hotmail.com,[2] Meiadjh@hotmail.com,[3] Nujud@outlook.sa,[4] hnodh-al5ald@hotmail.com,[5] Moooood25@hotmail.com, [6]k.aldahlan@uoh.edu.sa

ABSTRACT

This paper deepens into a serious problem in cyber security, which is measuring the awareness level of people about the cyber security and its related topics. This research will aim to explain the cyber security field extensively, and what does it implies and provides. Additionally, it will clarify why is it important in many aspects: personally, socially and politically. As well, it will cover the different cyber threats and their occurrence rate. Then, it will provide the steps which must be followed to protect the users against them. This research will adapt a quantitative method by conducting a questionnaire which will be adapted and built based on literature review of several papers and resources, and it will be aimed to a specific category which is the Ha'il university's students in the Kingdom of Saudi Arabia. And then, there will be another qualitative method used to understand the point of view of some specialist in the security, and to gain benefits from the experiences to address the problem properly. At the end, this research will provide steps to raise the knowledge of the society about the cyber security field; also it is recommended to design an education brochure which has the basic information and guidance for people who are not specialized in computer science, in order to make them more aware and careful with the internet world.

Keywords: Cybersecurity; Awareness; Saudi Arabia; Ha'il.

1. Introduction

The internet and computer technology has become a basic part of everyone's life, from all the different ages, in all the different fields and as well in all over the world. This technology has spread more than any other one.

People now use the internet in their daily lives through computers, smart phones, televisions, and many other devices for many purposes. Basically, it was used in communication process, as well in searching for different information and reading. But now it has evolved to be used in more than that and the best example is the situation which we live in now with the Corona pandemic. As an example, it has a significant role in the education process as in online classes, electronic books, and courses. As well in entertainment, a lot of individuals play games or watch movies online. Additionally, it is used effectively in commerce, in banks and its financial operations. And even the communication through internet has changed, it is now more advanced and there are lots of options with the existence of the social media applications.

Nowadays, even the governments use this technology to connect the different institutions with each other, as well as to provide services for the citizens. But on the other hand, as result of the wide usage of the internet, there are many possible dangers unfortunately. As long as we depend on internet, it will collect more data from us. And there are some malicious people who take advantage of this and do harmful actions for others; for example, by hacking into servers, stealing the private data of users, or impersonating them and many other threats.

For this reason, the cyber security now is considered as a very important field, it has a significant and critical role which is confirmed with the 2030 vision of the Kingdom of Saudi Arabia. This vision supports the use of information technologies and the enhancement of digital infrastructure, and this of course requires achieving cyber security which guarantees the protection of information and operations of the individuals in all the various fields.

This research was conducted to examine the level of awareness which a specific category of our society has about their security and privacy while using the internet, and to check if they understand the importance of the cyber security and the services it provides for them, and if they are conscious about the existence of adverse consequences of the absence of it.

1.1 The Background of the Research

As (Craigen et al., 2014) found many various definitions of cyber security depending on the context of the definer; after applying comparisons and analyzing them, they have defined it as: the combination of the used resources, structures and processes to provide the full protection for the cyberspace' systems. Additionally, (Von Solms & Van Niekerk, 2013) has shown that in cyber security, attacks are harmful and affect people as well the data. Whereas it is not the case in information security where the data is only affected. So, the cyber security includes the information security as a part of it, but the opposite is not true.

As (Singer & Friedman, 2014) defined the cyberspace as the whole environment which has the creation process of the digital data as well the used storage and the used sharing techniques; it includes the virtual elements and hardware which is the computer, along with the critical infrastructure of countries, which includes the information and data bases of all the significant sectors in the country.

Additionally, as illustrated by (Jones et al., 2018) that in Islamic world the technique of assessing the cyber-crimes is different because it is done corresponding to Islam. As well, the principals of Qur'an and Sunnah are used to create the cyber-crimes laws in Saudi Arabia. For instance, the privacy principle is included in Shariah law, it is instructed in the Qur'an to ask for permissions before gaining the access to others' possessions. This shows that it is required from Muslims to respect the individual's privacy and not to spy on them, so this principle is obviously applied in the cyber laws.

Cyber-crime covers the set of the various criminal activities which are done by the illegal using of computers, there are many different types of it such as cyber stalking, phishing and denial of service as defined by (Alqurashi et al., 2020). They also find it is important to provide a comprehensive law against the cyber-crimes. And specifically in the middle east, it is required to make these laws to be complied with Islamic laws such as the digital forensic which is set of the

used processes to preserve, identify, extract, and document the different computer evidence to be used in the court of law (Jones et al., 2018). Cyber-attacks cost the victims $114 billion annually (Jang-Jaccard & Nepal, 2014). They are less expensive, more convenient, and risky than physical attacks that is why cybercriminals commit them. Furthermore, due to the anonymous nature of the Internet attack, identifying and prosecuting them is extremely difficult. Malicious software attacks have traditionally exploited vulnerabilities in each layer during design and deployment. One example of attacks is malware which was created in the beginning as a means of exposing security flaws (Pande, 2017). There are several reasons make the attacker perform their activities, such as to feel the power and make accomplishes, to gain money and to fight for an idea of belief as (Ayofe & Irwin, 2010) found.

As (Vitunskaite et al., 2019) viewed cybersecurity is also important at the individual level in protecting personal data, pictures, files, videos, personal accounts, passwords, and bank accounts. And the internet is not restricted to adults only, children and adolescents in particular take a long time playing on the internet online games or browsing websites on the internet. That is why it is important to raise awareness by increasing knowledge of users as children. Educators need to educate students and choose the appropriate curriculum for each stage. Individuals of all ages must be prepared to defend themselves in the event of any electronic problems (Rahman et al., 2020).

As for the importance of cybersecurity in business, as (Yeboah-Ofori & Islam, 2019) stated; it enables employees to do their work easily and finish their procedures completely and safely which will increase production, also reduce costs and thus improve the business in general. If there is any compromised or tampered information, cyber security provides the ability to ease information retrieval, control and maintain business continuity and maintenance. As founded by (Wirth, 2016) in the medical field, the sensitivity of information of patients is high. The security process in the medical field is complex and includes the security of medical equipment, patient data or information. So, cyber security saves the lives of patients as well. (Callen-naviglia et al., 2018) illustrated that a financial technology increases the risk of attempted theft and threats. So, financial transactions and operations need high accuracy in organizing and operating in an exemplary manner in line with the importance of this field.

As stated by (Chandarman & Niekerk, 2017) the development of our technological world, attacks related to the internet are on the augmentation. However, in the future it is expected to increase everywhere due to the fact that technology has become a major thing in our world general. So, it is important to improve the knowledge, skills, behavior, and attitudes of individuals according to cyber security

As illustrated by (Thomas, 2018) the phishing represents a problem that is difficult to address due to the frequent exchange of information and messages, and sometimes it is difficult for trained and even smart employees to discover it. The researchers' (Hart et al., 2020) propose Riskio game which is played with attack and defense cards that cover a wide range of attacks and countermeasures from industry and government standards that make the game adaptable to a variety of contexts and scenarios; in order to provide participants an active learning environment. The current era is witnessing rapid and intense changes in technology, including both positive and negative ones; the negative changes had the strongest degree of influence, as found by researcher (Shalouch, 2018).

1.2 The Problem of the Research

With the presence of several daily operations which are achieved by the internet and electronic devices, people are more exposed to the various types of cyber-attacks, whether through hacking or viruses and others.

The problem is that not all users are aware of the risks of the internet and are not cautious. Therefore, the percentage of attacks will increase when their awareness decreases, and vice versa. This is a serious situation because it leads to many issues to the users of internet. Some of them might have a low adverse effect as for example hacking an email and using it. And others might have a high adverse effect as stealing the credit card information, or even worse as in hacking a monitoring camera or a smart door lock.

This research will attempt to cover the topic of cyber security broadly. Also, it will deploy a brochure containing the recommended several methods and techniques which must be followed to help users to protect themselves against cyber-attacks, and in order to enhance awareness in general.

1.3 The Objectives of the Research

The main objectives of this study are:

- Explain the main concepts of cyber security, as well to identify the importance of its application in real world.
- Measure the awareness of a certain group of society about the concept of cyber security and find out their familiarity to this concept.
- Interpret the causes of the resulted awareness' level of cyber security.
- Contribute to raising the level of awareness between the community members.

1.4 The Hypotheses of the Research

- This research is intended to assess the hypothesis that the level of awareness of the students regarding to the cyber security field is low.
- It is also designed to illustrate the importance of this field based on the literature review.
- Additionally, it is conducted to provide the possible causes of the resulting awareness level.

1.5 The Assumptions of the Research

This research will measure the awareness of a certain group about cyber security, which is the students of University of Ha'il; in all the various academic disciplines. It is assumed that most of them use the internet, laptop, and smart phones. And they are from the age group between 18-23 years old.

1.6 The Importance of the Research

This research will include basic and comprehensive information about cyber security, and what is its importance. Also, it will explain the relevance of this concept to our daily life, how strong it is, and how it will be more relevant in future since it is expected that the reliance on computers will increase. Also, the research will clarify what is the percentage of a part of society's awareness about cyber security, so it may help to take into account some procedures which will increase their security.

In general, computer science is a basic part of our life in the present time, and that will increase the importance of any research related to this science.

1.7 The Limitation of the Research

- Time of research:

The year 2020, the second semester.

- Place of research:

The university of Ha'il, the college of computer science and engineering.

- Targeted group:

The students at University of Ha'il in the Kingdom of Saudi Arabia.

2. Theoretical Framework of the study

2.1 General Definitions of Related Concepts

This was illustrated by (Craigen et al., 2014), who have the objective to define the cyber security term in a comprehensive manner, to be accepted to be used in all the different domains. They considered the absence of a unified definition of this science as an obstacle which prevents the achievement of cyber security consistently in the various areas, which affects the security of individuals in some means. This work is conceptual research which is based on a qualitative methodology; by interviewing some of the students, academics, and practitioners additionally with literature review. They have found many various definitions depending on the context of the definer, which are the following:

- The collection of mechanisms and techniques which are used for the purpose of providing the protection for the cyberspace from the cyber-attacks.
- The basic policies, guidelines, recovery management for protecting the systems, individuals, and their processes through the internet.
- Reducing the effects of the malicious attacks or viruses on the different devices and it also covers the tools which are used to detect these attacks and blocking them.

As a result, they have defined it as: the combination of the used resources, structures and processes to provide the full protection for the cyberspace' systems. In the paper conducted by (Von Solms & Van Niekerk, 2013), the objective was to explain the cyber security and the information security; as well, to clarify the difference between them. The authors used a qualitative methodology, by reviewing and reading the literatures about the two topics.

Information security: it is the process of preserving the confidentiality, integrity and availability of information and its resources. Some of people see that the information security has more properties than those three because the rapid changing nature of the computer world; so, they assume it includes preserving the data to be accurate, authentic, has saved utilities and possession to their owners and only them.

Cyber security: it is the combination of tools, concepts, policies, managements, actions, practices, and approaches to provide the protection to the cyber environment and individual's assets as devices, personnel, applications, and infrastructures. It guarantees the same three objectives of information security, but on a wider perimeter; it has an additional dimension which is the human being himself.

There are multiple cases which could not be included under the information security concept, as: cyber bullying: when someone uses the technology to embrace, harass, harm and be violent against other people; which could lead to a severe unfavorable impacts on them. So, it was concluded in cyber security, attacks are harmful and affect people as well the data. Whereas it is not the case in information security where the data is only affected. So, the cyber security includes the information security as a part of it, but the opposite is not true.

As (Singer & Friedman, 2014) discussed in his book the cyber space in general and its related topics, it shows how our lives are surrounded by computers, and how it is included in all the different details in our daily operations such as clocks, coffee machines, smart ovens, cars, work area, education area and even in entertainment area sometimes.

In the past computer usage was extremely limited, but now it is used intensively. For instance, as average there are 40 trillion e-mails are sent in a year. And there are 8.7 billion devices connected to internet such as: fridges, medical devices, locks and many others. This book has used six years old statistics, so imagine these numbers now.

The authors have mentioned that the cyber space term is not easy to define, because it is globally used, and its boundaries are not easy to recognize and drawn. But eventually, it is defined as the realm of the connected computer through the networks, and the users who store and share information. It is the whole environment which has the creation process of the digital data as well the used storage and the used sharing techniques. It does not only include the virtual elements, but it is also more broad and covers the hardware which is the computer, along with the infrastructure and systems. Additionally, it includes the critical infrastructure of countries, which includes the information and data bases of all the significant sectors in the country such as agriculture, food industries, banks, healthcare sector, power, transportations, and water as well.

The paper written by (Alqurashi et al., 2020) aimed to investigate the status of the cyber-crimes and the forensics in the region of the middle east, by taking the Kingdom of Saudi Arabia as a case study; they have followed a qualitative approach to explore the challenges of the cyber-crimes, as well understanding the impact of them on people.

Firstly, the term cyber-crime must be defined; it covers the set of the various criminal activities which are done by the illegal use of computers. It surely has strong effects on people.

It is important to provide a comprehensive law against cyber-crimes, but it is not sufficient alone and it is not the only factor needed to avoid or reduce the occurrence of them. Another factor which has a significant role is providing the appropriate education for individuals about this aspect. It is one of the most effective ways to decrease the rate of cyber-crimes. In the middle east, almost all of the countries have their own electronic laws; and it is required to make these laws to be complied with Islamic laws. In Saudi Arabia, there is 15.8 million users of internet. Additionally, almost all the government transactions and operations are involved in computers and internet. And one of the most popular examples is the cyber-attack on the Saudi oil company Aramco, there was more than 30 thousand computers attacked by a virus in 2012; as a result of this incident, many of the information had lost and computer drives had destroyed. The goal of that attack was to intercept the production of oil.

The paper of (Jones et al., 2018) paper followed a qualitative methodology to present how are the principals of Qur'an and Sunnah are used and presented in the cyber-crimes laws in Saudi Arabia. For instance, the privacy principle is included in Shariah law, it is instructed in the Qur'an to ask for permissions before gaining the access to others' possessions. This shows that it is required from Muslims to respect the individual's privacy and not to spy on them, so this principle is obviously applied in the cyber laws. The digital forensic is defined as the set of the used processes to preserve, identify, extract, and document the different computer evidence to be used in the court of law. There are several steps in the process of digital investigation. As well, it is important to understand in Islamic world the technique of assessing the cyber-crimes is different because it is done corresponding to Islam.

2.2 Types and Reasons of Cyber attacks

Computer networks and IT solutions have become increasingly important in today's society, economy, and critical structures. As our reliance on technology grows, cyber-attacks can become more devastating. Cyber-attacks cost $ 114 billion annually, according to Symantec's April 2012 Cyber Crime Study. According to a survey conducted by Symantec, 69% of people had suffered a cyber-attack (Jang-Jaccard & Nepal, 2014).

Cyber-attacks are less expensive, more convenient, and risky than physical attacks. Cybercriminals just need a computer and access to the Internet. They do not need a lot of money. They are also unconstrained by geography or distance, allowing them to invade any nation. Furthermore, due to the anonymous nature of the Internet attack, identifying and prosecuting them is extremely difficult. Given how appealing attacks on IT systems are, it is expected that the number and sophistication of cyber-attacks will continue to rise in the future.

Malicious software attacks have exploited vulnerabilities in each layer during design and deployment. Understanding the issues surrounding various cyber-attacks, as well as designing defensive strategies that ensure security, is what cybersecurity is all about. To achieve primary security goals. The CIA's three main security goals are:

- Confidentiality: the protection of sensitive information from being disclosed to unauthorized people or systems.
- Integrity: the prevention of unauthorized alteration and deletion of data. (Abomhara & Køien, 2015).
- Availability: the insurance that the systems in charge of delivering, storing, and processing data can be accessed by legitimate users anytime they need it.

Accountability is applied on top of them to punish any bad conduct. Figure 1 illustrates this.

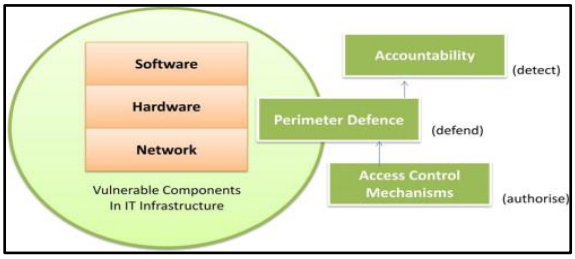

Figure 1: The vulnerabilities and defense strategies in existing systems

The malware was created in the beginning as a means of exposing security flaws or demonstrating one's ability to write these programs. When malware is installed on a victim's computer, cybercriminals can exploit a variety of flaws in the victim's system. Most of the time, cybercriminals use existing malware signatures to exploit bugs, but they also use emerging technologies (such as social media, cloud computing, and smartphone technology) to reach victims quicker and more effectively. It is primarily used to steal personal, financial, or business details. In 2017, there were 26 million new malware reports. (Pande, 2017). Figure 2 describes relative proportions of the types of new malware samples identified in the second half of 2012 reported by the Anti-Phishing group.

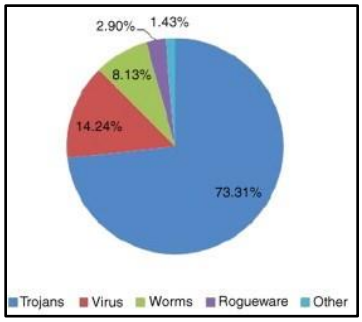

Figure 2: The types of malware and mediums to spread them

Spam is the practice of sending unwanted and offensive messages to millions of people. According to the Messaging Abuse Action Study, spam was found in 88-92 percent of emails sent in 2010. The explanation for this is that spam was a new challenge in 2010 by (Jang-Jaccard & Nepal, 2014). Phishing is a technique used by hackers to acquire personal information such as passwords, usernames, or credit card numbers by impersonating a trustworthy individual. The majority of phishing scams work by tricking users into visiting a malicious website (Renu & Pawan, 2019). A cybercriminal may be from inside or outside the company that is the target of a cyber-attack. An internal intrusion known as a network or computer system attack by an individual with approved access to the system is one form of cybercrime. When an external individual attacks the company, this is referred to as an external attack. A company that is the target of a cyberattack not only loses money but also loses its credibility (Renu & Pawan, 2019). Cyber-attacks are graded as follows, depending on the attacker's maturity level:

a) Unstructured attacks: These are carried out by amateurs who have no particular reason to carry out a cyber assault.
b) Structure attack: These attacks are carried out by people who are highly trained, experienced, and motivated.

There are many reasons why cyber criminals commit these crimes, and the most popular reasons are: (Ayofe & Irwin, 2010).

- Confession: this is committed by people who want to feel like they are among a group of powerful men in society. They do not mean to harm anyone in particular. They fall into the category of idealists who just want to be in the spotlight.
- To make money: this is committed because of money greed, by tampering the information on the network, especially e-commerce and electronic banking data information, with the aim of committing fraud and defrauding the money of unsuspecting clients.

- Fight: to fight for what they believe in; the most dangerous cause of cybercrime is to cause a threat or harm that negatively affects its recipients. These are cyber terrorists who imply the belief that they are fighting for a just cause, and thus have no interest in who or what they destroy in their pursuit of their goals.

2.3 Importance of Cyber Security

With rapid development in all over the world, the technological development requirements to keep pace with this development, specialist of safety said to achieve this development goals and workers or business in all its aspects as (Vitunskaite et al., 2019) mentioned. Although the computer and the internet facilitate a lot of business as. On the other hand, it presented many negatives, which are resulted from shortage of awareness between the users of internet until they become victims.

The importance of cybersecurity lies in protecting users, companies, society and even governments from various types of these threats. Cybersecurity is also important at the individual level in protecting personal data, pictures, files, videos, personal accounts, passwords, and bank accounts. In terms of society, it protects from social engineering and targeting social behavior.

The internet is not restricted to adults only, children and adolescents in particular take a long time playing on the internet online games or browsing websites on the internet, which may contain several threats. That is why it is important to raise awareness by increasing knowledge of users as children. Educators need to educate students and choose the appropriate curriculum for each stage, also interest in a culture of cybersecurity to reduce digital illiteracy as suggested by (Rahman et al., 2020). Individuals of all ages must be prepared to defend themselves in the event of any electronic problems.

As for the importance of cybersecurity in business, as (Yeboah-Ofori & Islam, 2019) stated; it has great importance in the Supply Chain; as it enables employees to do their work easily and finish their procedures completely and safely, which will increase production, also reduce costs and thus improve the business in general. The cyber security doing the mutual credentials that will avoid the manipulating and changing in the business by third party.

By using the Cyber Physical Systems (CPS), it carries out the process in an integrated manner to obtain the information in the right way without any interference or threat to complete the business processes, when we use cyber security to restrict access to that business, we can uncover threat attempts, potential attacks, manipulations and breaches that are sure to affect business continuity, quality, and reliability. And if there is any compromised or tampered information, cyber security provides the ability to ease information retrieval, control and maintain business continuity and maintenance. This will increase the security controls to ensure the flow of work, the achievement of the objectives, the minimization of risks, the means of protection, the confidentiality, and the integrity of the information. As found by (Wirth, 2016) when we look in the medical field, the sensitivity of the patient's information is high. And the security process in the medical field is complex and includes the security of medical equipment, patient data or information, and the perception of users at the same time for accurate and reliable handling of any device connected to the network. The importance of cyber security lies in preserving these devices, as it goes beyond that until its arrival saves the lives of patients.

There are many requests to easily use banking and e-commerce services to keep pace with this progress as (Callen-naviglia et al., 2018) illustrated. This demand affects the company to create a financial technology (Fin Teach), as it will change and develop financial methods with the technological development. With this development in the financial world, it increases the risk of attempted theft and threats. Financial transactions and operations need high accuracy in organizing and operating in an exemplary manner in line with the importance of this field. It is the use of the Regulatory Technology System (Reg Tech), and it works on the organization, accuracy and preparation of financial reports necessary to maintain the financial system, and it tries to advance in dealing with financial technology.

Cyber security gives the correct digitization of financial operations and continuity of their work and keeping them protected from any manipulation or theft. It is developing safety lockers to protect this money and information. It has brought many benefits that improve businesses such as increased efficiency, reduced costs and preservation of the environment.

2.4 How to Prevent Cyber Attacks

As stated by (Chandarman & Niekerk, 2017) the development of our technological world, attacks related to the internet are on the augmentation. However, in the future it is expected to increase everywhere because technology has become a major thing in our world general.
This study attached to the educational institution in South Africa and a questionnaire was conducted on knowledge of cybersecurity, self-perception of cybersecurity skills and the actual behavior of it as well, the study followed an exploratory approach and was related to the student's knowledge of cybersecurity, the student's online uses and students 'attitudes towards this information security. The topics were related to: password security, cyberbullying, phishing, malware, identity theft, downloading, sharing and use of pirated content. And the variables are related to: knowledge, self-perception of skills, actual behavior and skills, attitudes.

The results of this study varied in percentages. With regard to pirated content, students here reported most of the skills and behaviors, indicating that they participated in piracy, despite their knowledge that it is wrong attitude. As for cyberbullying, although students reported self-perceptions of skills and manners to avoid cyberbullying conduct, for instance, posting messages over the Internet, most students gave us reactions indicating that a potentially harmful attitude toward posting abusive images and messages. As for passwords, students are all unanimous about not remembering complex passwords, so they use simple passwords, which is a potentially harmful situation. The aspects of the study took many variables and opinions differed, but the points above clarified the orientation of most students and the similarity of their answers concerning that.

As illustrated by (Thomas, 2018) phishing is one of the most difficult challenges in the field of cyber security, it represents a problem that is difficult to address due to the frequent exchange of information and messages,. It is also relevant to social engineering andit is difficult for trained and even smart employees to discover it. It makes crime commission the largest area, and researchers are exploring several ways to address this problem, including user education and awareness. The purpose of this study was to conduct interviews with specialists in the field of cybersecurity to get a better view of preventing users and employees from succumbing to this attack. It was found that the problem is related to users is the lack of information related to human psychological factors.

This clarifying by (Conteh & Schmick, 2021) study aimed to assess weaknesses in the information technology infrastructure of companies and institutions, which contain hardware and software systems, local and wide area networks, corporate networks, internal networks, and their uses of the Internet for cyber interference. The study discussed the role of social engineering in network intrusion and electronic theft and discusses the reasons for the rapid spread of electronic crimes. The study also indicated that the human factor will always be a security vulnerability.

This is stated by (Humayun et al., 2020), they dealt with identifying and analyzing common vulnerabilities in cybersecurity, and a systematic mapping study was conducted. 78 preliminary studies were identified and analyzed. The infrastructure targeted in the applications, the results showed that the security methods so far target security in general only and that the solutions presented in these studies require more experiments, experimental verification, and real implementation, as the studies here have targeted very few common security vulnerabilities such as phishing and denial of service.

This cleared from (Senarak, 2021) study which attached to the massive integration of port operators with electronic technology into port activities, making this digitization a major weakness of the emerging cyber threat. It developed a concept and also developed three methods of cleaning cybersecurity in ports _meaning human factors and infrastructure_.
Piracy, cybercrime, electronic espionage, terrorism, and electronic warfare have all validated the relationships between cyber security in ports and electronic threats. The study presented ways to prevent these cyberattacks, as providing training and education for employees in the port, keeping important information safe, and other preventive measures to reduce the risks of cyber threats.

2.5 The Cyber Attacks Future Consequences

Researchers (Yaacoub et al., 2020) aimed to get to know CPS security, they are designated as essential components of the industrial Internet of Things (IoT), also they are based on the integration of cyber and physical systems which exchange many types of data and sensitive information. The development of CPS is being carried out by researchers and manufacturers, they consist of the combination of various interconnected systems with the ability to monitor and manipulate real IoT objects and processes. CPS includes three main central components: sensors, aggregators, and actuators. They are embedded in different systems such as power transmission systems, communication systems, and many.

CPS threats can be classified as cyber or physical threats, and if combined, these can result into cyber-physical threats, which are difficult to mitigate and overcome in the absence of the right prevention and defensive countermeasures.

- Physical attacks: infected items, abuse of privilege, wire cuts, fake identity, malicious third-party software provider, physical breach, abuse of privilege, social engineering.
- Cyber-attacks: eavesdropping, cross-site scripting, SQL injection, password cracking, phishing, replay, DoS/DDoS, malicious third party, watering-hole attack, malware.

There are several risks associated with CPS security attacks. Also, the CPS insurance is not a direct task, and plans have been introduced to protect CPS domains from attacks. To ensure trust between IoT and CPS should consist of various multi-factors. All of which are combined to form a well-designed and trustworthy system. If this condition is satisfied, a perfect CPS mechanism is

achieved as a result. In research of (Gunduz & Das, 2020), the aim was to supply a deep understanding of cyber-security vulnerabilities and solutions and the security of smart grid applications. Smart grid has a complex infrastructure. It is an electricity market that enables to generate, store energy, and shift load for customers.

One of the significant disadvantages of smart grid development is the cyber security issues involved in, which slow down the progress of smart grid applications. Smart grid cyber security issues include ensuring the CIA triad of the control systems. Cyber security objectives of smart grid must have precautions securing information with CIA triad. These key security principles must be met in smart grid systems. Data must be protected from unauthorized access or disclosure, it must not be tampered by anyone or anything in the system, thus, the data must not be changed an unauthorized or undetected manner. Also, integrity means to maintain and ensure the truth of the data, it must have secure real-time monitoring system to smart grid. And the information must be available to authorized parties in the smart grid when needed without compromising security, the DoS attacks that lead to blackouts must be prevented.

There are different vulnerabilities and each one has different characteristics. The applications might be exposed to distinct cyber threats that can damage from a low to a high level. The correct identification of the type of security threats and vulnerabilities enable to determinate proper countermeasures. In general, cyber security against sophisticated cyber-attacks is a major challenge because of new attack tactics are continuously discovered, existing ones keep evolving, and most of the IoT devices do not have stringent security protocols and secure encryption mechanisms. The researchers' (Hart et al., 2020) aim was to propose Riskio, a board game where participants build their knowledge on cyber security attacks and defenses by playing both the role of attackers and defenders of critical assets in a fictitious environment. The game is played with attack and defense cards that cover a wide range of attacks and countermeasures from industry and government standards that make the game adaptable to a variety of contexts and scenarios.

In order to provide participants with an active learning environment, the design of the game is based on building learners' knowledge through experiences. Players reflect upon their attack and defend strategies, discuss between each other's, and providing immediate feedback on the correctness and effectiveness of their strategies.

The effectiveness of this game is to contribute to knowledge acquisition and retention. And increase the ability to recall knowledge after some time has passed from the training. It also can support a variety of educational and training activities in academic and industry settings. It is also proposed to involve employees with limited security expertise, with a particular focus on threat modelling, risk assessment, security requirements elicitation, and secure coding. The goal of the researcher (Shalouch, 2018) is to identify the electronic piracy in cyber space which is the growing threat to the security of countries.

The current era is witnessing rapid and intense changes in technology, including both positive and negative ones; the negative changes had the strongest degree of influence, especially in the area of undermining the security of states because of the spread of cyber-attacks, which necessitated the systems.

Electronic piracy affects the emergence of new patterns of conflict international. The world today is witnessing an electronic race in the emergence of new electronic weapons, in the context of a response. So, the militarization of cyberspace is needed especially in modern societies which have become increasingly dependent on technologies. Cyber security forms an essential part of any international defense security policy, especially because there are more than 130 countries which allocate facilities for cyber warfare within the national security teams. The risks in this area lies in the difficulty of determining the identity of the entity that carried out the cyber-attack, as well as the absence of international legislation and institutions that establish the activities under international law, which means the inability to legally prosecute them.

The importance of the (Abed Ali & Rabab, 2020) research lies in the fact that it sheds light on the increase in cyber-attacks in recent times, with the difficulty of determining their implications and the difficulty of determining the party that issued these attacks, in addition to the scarcity of Arabic resources dealing with cyber-attacks and the legal regulation of them, due to the modernity of such topics. Additionally, the lack of a unified definition of cyber-attacks due to the lack of a definition of the cyber space in which these attacks occurred. It also was concluded that the emergence of a new field for war, which is cyber, which has been increasingly resorted to recently. This is because it is less cost and more difficult to identify the aggressor, which results in the most serious violations of international humanitarian law in this type of war.

3.The Research Methodology

In this research, the considered problem or the question needs to be answered is the following, what is the awareness level of the students at University of Ha'il. So, for the purpose to answer this question, it is needed to gather information from a sample of the students from various colleges; the proposed technique to collect them is by conducting a questionnaire. The questionnaire will be conducted by reviewing many resources and the questions will be tailored according to our environment and needs (Al-Janabi & Al-Shourbaji, 2016; Aljohani & Elfadil, 2020; Javed, 2020; Sattler, 2019).

It is the first method to use, it will include several questions to identify the students' reaction by providing contexts of multiple situations of different cyber-crimes with the possible responses, to see how the individuals would react to these cyber-crimes, in order to measure the level of awareness they have. As well, it will measure their understanding of several concepts of cyber security, and also to see if they already perform some of the correct security procedures or not.

After that, the statistics will be analyzed to decide if the level of awareness is high or as it assumed in the beginning of the research, which is low or maybe medium. And we will analyze the reasons that lead to that level with the help of other further methods. The other technique will be used, is conducting an interview with some of the stakeholders or responsible managers in the National Cybersecurity Authority in Saudi Arabia. By applying this method, we aim to gather more information to understand what are the factors and reasons which lead to the stated cyber security awareness level.

Then, another interview will be conducted with the dean of the computer science and engineering college and dean of admission and registration; to understand their point of view about the reasons which lead to that rate.

At the end, with the help of our research supervisor, we will attempt to conduct a brochure which will provide the basic principles to understand cyber security. Additionally, it will provide the steps to be followed by users to be more secure in cyber space and raise the level of awareness in general.

3.1 First method – the Questionnaire

- What do you think about cyber security?

- It is the security against hacking the information system of the country specially which has sensitive information.
- It is the security against the cyber-crimes and attacks, viruses and their threats, sniffing on communication for all users.
- All of the above.

- Do you check for viruses when you download a file or open an email attachment?

- Yes.
- No.

- What is the strongest password from the following?

- Norasaleh
- 11223344
- Qwerth
- Rd56&G

- When you receive an email from the bank you deal with stating that your account needs verification because the installation of a new system, you are required to enter a specific link and provide personal information, you must respond within the 24 hours, or your bank account will be blocked and frozen. What will you do?

- Click on the link and provide the required personal information to handle the problem without getting account freezing.
- Ignore the link, it appears to be a scam.
- Contact the bank to check if this is true.

- Do you use the same password for all your accounts in different websites?

- Yes.
- No.

- Which one of the following statements describe the phishing attack?

- It includes the unwanted requests (spam) to manipulate the recipients into revealing their personal information.
- It includes hacking the devices to steal information.
- I do not know.

- Do you share your personal and sensitive information on your social media account?

- Yes.
- No.

- What is the difference between https and http in URL?

- The link which includes https provides encryption of information, and the website includes http does not provide it.
- https is a new version of http.
- I do not know.

- Do you download free content and software from untrusted websites?

- Yes.
- No.

- What do you think about this statement: turning off the GPS function from your mobile phone, this act increases your privacy.

- The statement is true.
- The statement is false.

- What is social engineering?

- A social orientation to organize the internet.
- Fraud and tricks to reveal private information of internet users.
- New theory in management.

- Do you read the user agreements of the software before you accept them?

- Yes.
- No.

- If your business email account has been hacked, what would you do?

- Change your password.
- Inform the organization.
- All of the above.

- Do you check the updates for your antivirus software in a regular manner?

- Yes.
- No.

- The mouse pointer on your screen begins to move by itself and click on the files on the desktop. What will you do?

- Disconnect computer from the internet.
- Shut down your computer.
- run antivirus program.

- Do you transfer money to your friends when they ask you through a message?

- Yes.
- No.

- What is the security protection should be available when using the internet?

- Antivirus, spyware protection program.
- Controls to protect adolescents from entering inappropriate sites.
- All of the above.

- Do you use public networks with password to do some sensitive operations such as accessing your bank account?

- Yes.
- No.

- What do you think about cyber-attacks?

- They are harmless and cannot damage your data, so antivirus software is waste of money.
- Only those who visit the restricted sites will be affected by attacks.
- Internet attacks are very dangerous, so it is worth taking the utmost caution.

3.2 Second Method – the Interview

Q1: What certificates do you have obtained?
Q2: Do you think that the majority of people around the world are now aware of cyber-attacks? Or is there still a large percentage of ignorance in this field?
Q3: With regard to the Saudi society in particular, do you think that they need awareness of cyber risks, or do they have an adequate awareness level? And what are the reasons, in your opinion, of low or high percentage?
Q4: In particular, do you think that the students of the University of Hail (in all majors) are aware of the risks resulted of cyberattacks, or the awareness is limited to students of the computer science and engineering college regarding to their specialization?
Q5: Do you think the students are aware of the legal penalty for using unlicensed software?
Q6: What do you think are the most dangerous and widespread cyber-attacks at the moment?
Q7: What is your method to educate your children in general when they use the internet and electronic devices, and are there techniques which you use on their devices to protect them?
Q8: How do you think the field of cyber security will be after ten years from now?
Q9: Do you have advice to students in particular, to society in general, and to us, your students in the field of cyber security?

4.The Result and Discussion

4.1 The Questionnaire Result:

The following chart presents the statistics of the gathered data from responses on the questionnaire; for each question it is indicated the percentage of the selected answers by the sample who answered that questionnaire.

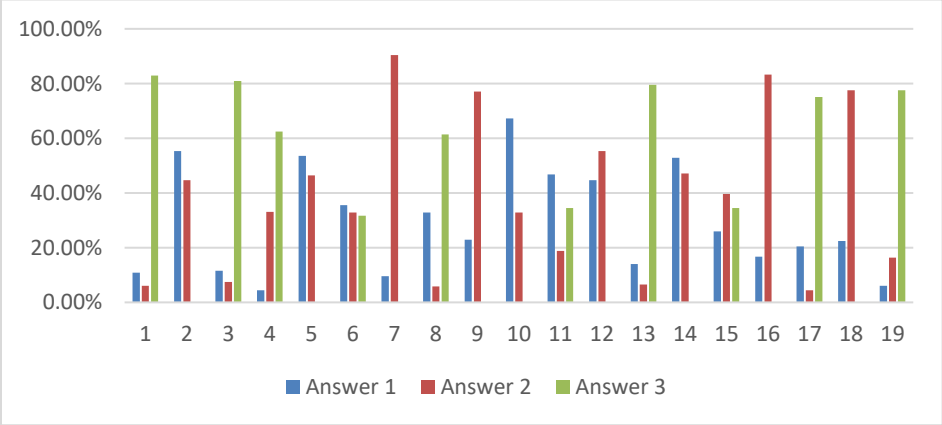

Figure 3: The statistics of answers

The questionnaire was sent for the students at University of Ha'il; it was available for one week and it gathered 293 responses from students with different majors.

- Most of them are aware of the correct meaning of cyber security.
- In the different contexts provided in the questionnaire; the answers were mostly correct.
- On the other hand, there was a shortage in understanding the meanings of different concepts related to cyber security.

As the chart shows, it has found that most of the students are only aware about the basic and general concepts, such as the meaning of the cyber security, the risk of cyber-attacks, and what are the security methods must be available while using the internet. But in the more specific concept, there were less awareness; such as the meaning of the social engineering threat, the difference between HTTP and HTTPS in the websites, and as well in understanding the capabilities of attackers when they reach any simple connection to their devices.

In fact, many of them understand the correct actions or procedures which leads to high security and protection; such as in checking the files for viruses, not sending money to friends who asked through a message, and in understanding what is the correct form of a strong password.

But there is still a level of shortage in awareness because most of them use the same password for different websites and do not read the agreements of software when they download them. The response is in different cases and contexts where a security risk is raised was not predicted, such as in the case where they receive a message from bank, hacking a business email, and action performed when it is suspected that an intruder taking control of their computers.

Generally, the questionnaire was conducted to measure several aspects. It is intended to measure their understanding of the main concepts of the security. As well, it is aimed to measure how many correct procedures they follow to increase their prediction in the cyberspace. Additionally, one of the goals of this questionnaire is to get an overview about their knowledge in some of the strongly related topics to cyber security. As well, to indicate if they take the correct responses and reactions when they are in a risk situation.

The following chart shows the rate between the overall correct answers which are indicated by the number (1), and the overall incorrect answers which are indicated by the number (2).

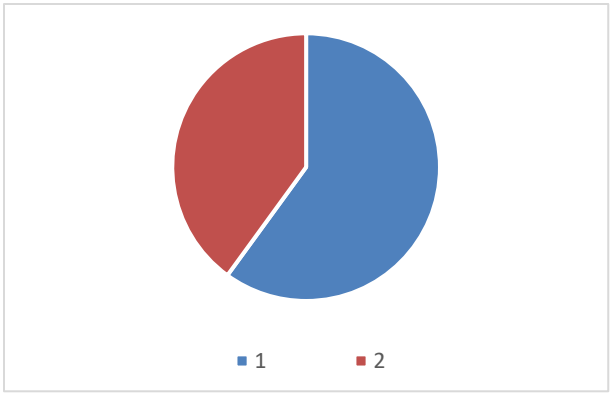

Figure 4: The rate of answers

As calculated, 60% of the answers were correct. So, this shows the assumption of this research was not correct; because this percentage indicates the level of awareness in cyber security of the specific category is not low but medium. This rate is acceptable, but it is not the optimal or excellent rate which indicates their awareness is high; So, it is preferred to conduct any method to increase their awareness.

As the results found in the literature review and the analysis according to our point of view, the awareness level is affected by many factors such as:

- The lack of Arabic resources in the field of cyber security.
- There is a high percentage of internet users belong to children and elderly people; these two categories do not fully understand the nature of internet world; hence they are facing several challenges in it.
- Lack of education provided to individual in that specific category; people around do not educate them and explain the basic steps to them to be secured.
- The existence of many people who are willing to attack, for several intents.

As inferred from the most incorrect answers in the questionnaire, there are many steps that must be taken into account in order to act securely through the cyberspace; which are:

- Password is one of the most important things that keep your privacy high. It must consist of upper and lower case letters, symbols and numbers, for example: AsamtG89&, and it must not be used in different sites.
- Protecting your smartphone, pay close attention in downloading applications on it, and also disable Bluetooth and location services except in necessary cases.
- Connecting to public Wi-Fi should be avoided, as they can easily hacked. Always use a private network with an access code to avoid cyberattacks.
- Be careful in social media and do not accept request from people you do not know and beware of suspicious messages.
- Be careful not to give your private information to anyone, such as the bank card number, password and access code for devices.
- The operating systems and software must be updated. The updates include security patches to fill loopholes that may be exploited by attacker.
- Not opening untrusted links received from social media, it might be a method used by attackers to gain access.
- In online shopping, only use secure websites, to avoid cyberattacks especially when the website has unbelievable offers.
- Be aware, it is preferable to use (https) websites instead using (http) ones. and if it is necessary, do not enter sensitive data, bank data, password, or e-mail.

4.2 The Interview Result:

This interview was conducted to be provided to several people, in order to gain more precise interpretation and analysis. And to get valuable feedback from their experience.

Unfortunately, there were not any responses so the result and discussion will be limited on the questionnaire responses only.

5. Conclusion of the study

The awareness level of the targeted category is medium which contradicts with the assumption of the research as shown by the statistics analysis of the questionnaire. This level is resulted from many reasons; but it is able to be increased through several practices; which is preferred because cyberspace is widely used, and it will be more dependable in future.

In order to increase the level of awareness of the selected sample, and also to a wider range of people; it is recommended to provide one of education sources; so, this brochure is designed in both languages (Arabic and English). It presents the basic concepts as well as providing the steps to be more secure in cyberspace.

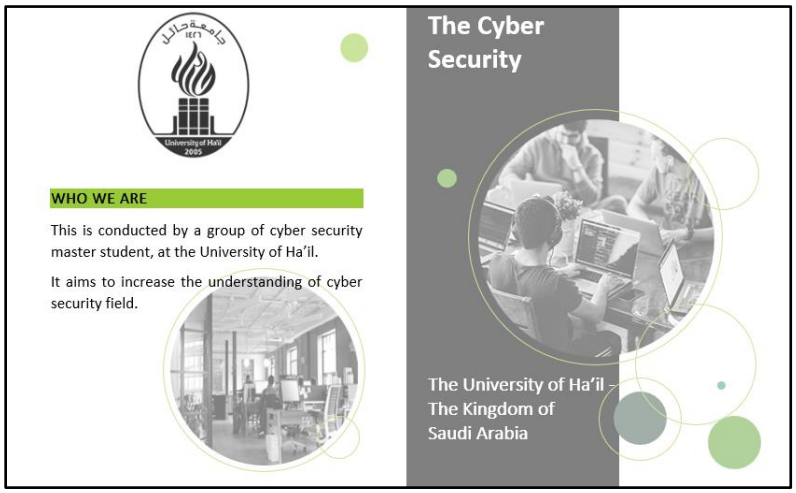

Figure 0: The English version of brochure – 1

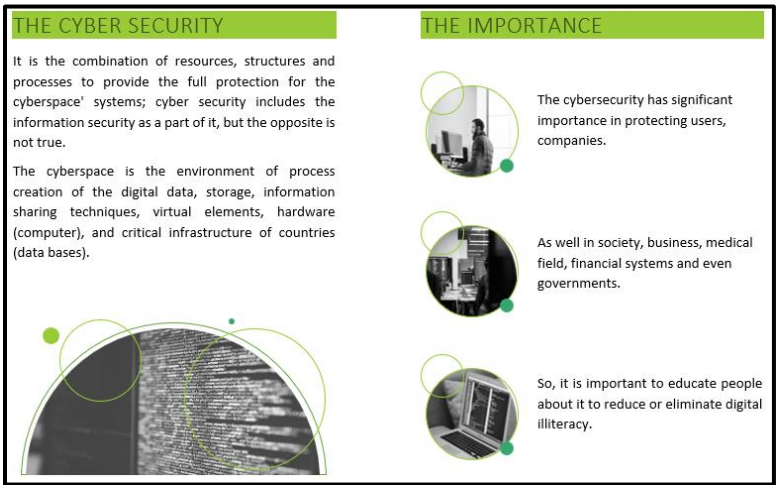

Figure 6: The English version of brochure - 2

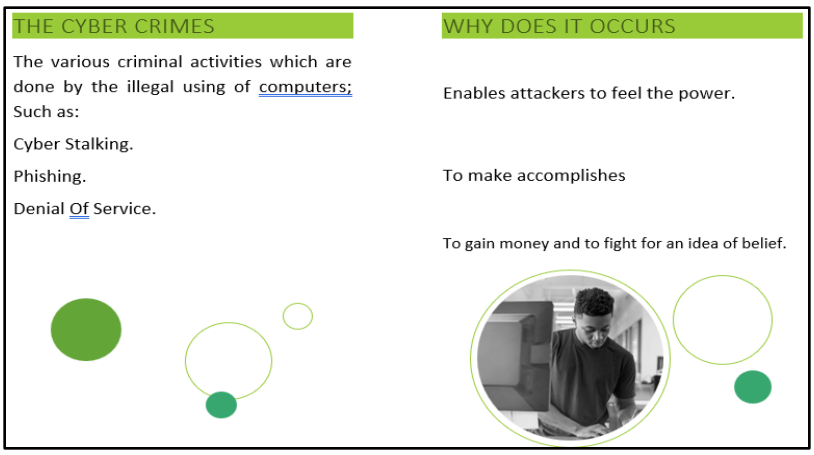

Figure 7: The English version of brochure – 3

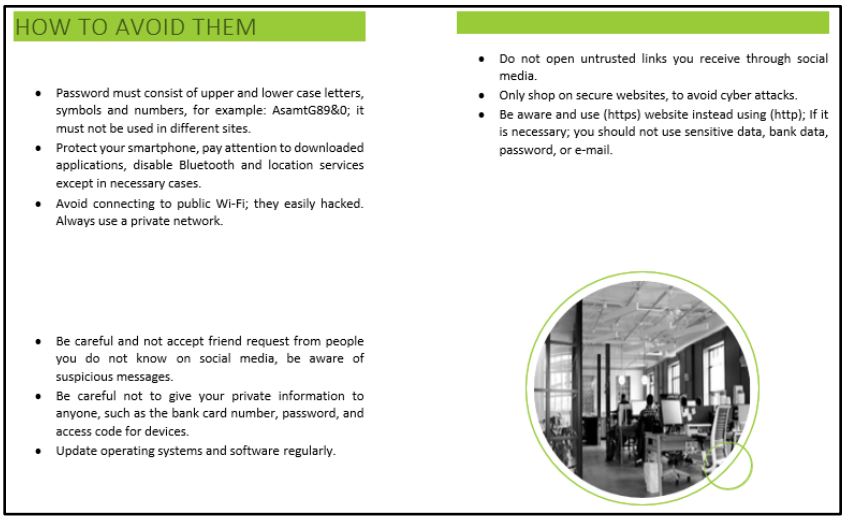

Figure 8: The English version of brochure – 4

Figure 9: The Arabic version of brochure - 1

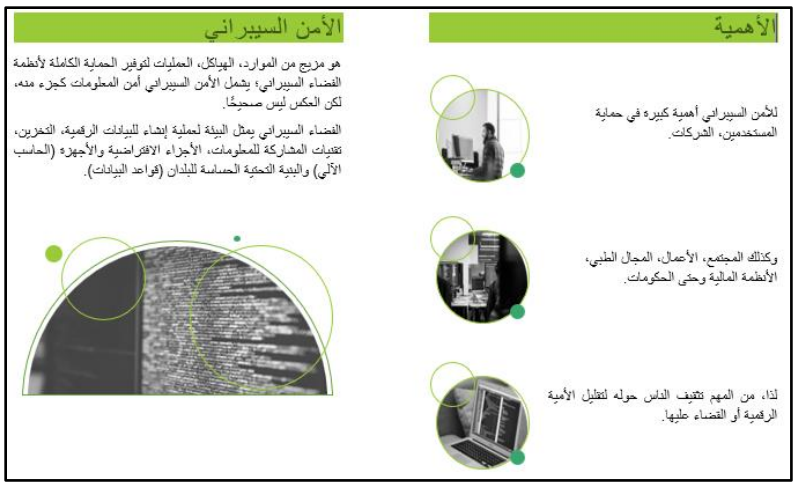

Figure 10: The Arabic version of brochure – 2

Figure 11: The Arabic version of brochure – 3

Figure 12: The Arabic version of brochure – 4

REFERENCES

Abed Ali, H. K., & Rabab, A. M. (2020). Legal regulation of cyber-attacks on facilities with dangerous forces. *Kufa Legal and Political Science*, *1*(47), 107–127.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information and Knowledge Management*, *15*(1). https://doi.org/10.1142/S0219649216500076

Aljohani, W., & Elfadil, ; Nazar. (2020). International Journal of Computer Science and Mobile Computing Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University. *International Journal of Computer Science and Mobile Computing*, *9*(6), 141–155. www.ijcsmc.com

Alqurashi, R. K., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2020). Cyber Attacks and Impacts: A Case Study in Saudi Arabia. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(1), 217–224. https://doi.org/10.30534/ijatcse/2020/33912020

Ayofe, A. N., & Irwin, B. (2010). Cyber Security: Challenges and the Way Forward. *Computer Science & Telecommunications*, *29*(6).

Callen-naviglia, J., Bank, P. N. C., & James, J. (2018). Fintech, Regtech and the Importance of Cybersecurity. *Issues In Information Systems*, *19*(3), 220–225. https://doi.org/10.48009/3_iis_2018_220-225

Chandarman, R., & Niekerk, B. Van. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational. *The African Journal of Information and Communication (AJIC)*, *20*, 133–155.

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*, *6*(23), 19–31. https://doi.org/10.4018/978-1-7998-6504-9.ch002

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Defining cybersecurity. Technology Innovation Management Review*. *4*(10), 13–21.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers and Security*, *95*, 1–18. https://doi.org/10.1016/j.cose.2020.101827

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171–3189.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Javed, A. (2020). *Security awareness quiz questions*. John Opdenakker. https://johnopdenakker.com

Jones, A., Alanazi, F., & Menon, C. (2018). Sharia Law and Digital Forensics in Saudi Arabia. *Journal of Digital Forensics, Security and Law*, *13*(3). https://doi.org/10.15394/jdfsl.2018.1568

Pande, J. (2017). Introduction to Cyber Security. *Technology*, *7*(1), 11–26.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Renu, & Pawan. (2019). Impact of Cyber Crime: Issues and Challenges. *International Journal of Trend in Scientific Research and Development*, *3*(3), 1569–1572. https://doi.org/10.31142/ijtsrd23456

Sattler, J. (2019). *10 Cyber Security Awareness Month questions to ask your friends*. F-Secure. https://blog.f-secure.com

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. *Asian Journal of Shipping and Logistics*, *37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001

Shalouch, N. (2018). Cyber piracy in cyberspace" The growing threat to state security. *Journal Of Babylon Center for Humanities Studies*, *8*(2).

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*.

Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management*, *13*(6), 1. https://doi.org/10.5539/ijbm.v13n6p1

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Computers and Security*, *83*, 313–331. https://doi.org/10.1016/j.cose.2019.02.009

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wirth, A. (2016). Cyberinsights: The importance of cybersecurity training for HTM professionals. *Biomedical Instrumentation and Technology*, *50*(5), 381–383. https://doi.org/10.2345/0899-8205-50.5.381

Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, *77*(103201), 103201. https://doi.org/10.1016/j.micpro.2020.103201

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future Internet*, *11*(3). https://doi.org/10.3390/fi11030063