Research Article

Exploratory Study to Measure Awareness of Cybercrime in Saudi Arabia

Nourah Almrezeq[a], Faiez Alserhani[a,] Mamoona Humayun[a,*]
College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract : Saudi Arabia is one of the fastest-growing nations in respect to using technology and the Internet. In recent years, the usage of these innovations has grown significantly. There's a relationship between increasing Internet usage and rising cybercrimes. Although the spread of various protection techniques with different levels of security, there is a lack of application and public awareness. Protection techniques alone are not sufficient to confront cybercrimes, so awareness of cybersecurity is considered one of the most important reasons for reducing cybercrimes. Saudi Arabia is strengthening its interest in the field of cybersecurity. However, there is still an urgent need for research and investigation in awareness of cybersecurity and cybercrime. This study has been applied to students of Jouf University. The study has targeted a group of students who are not fully aware of digital crimes related to technology and the Internet. The study has shown a significant increase in awareness of cybersecurity. However, there is still a group of students with little or absence of awareness of understanding of cybersecurity. The survey analysis results have shown that for most of the participants who encountered cybercrimes, the respondents didn't inform about the incidents to the local authorities and law enforcement. The majority of the participants emphasized the importance of enriching the digital content for the public with information about cybercrimes and how to deal with it according to local legislation. Literature review and survey results analysis show that there is a need for a framework that may help in developing awareness among Saudi's residents about cybercrimes.

Keywords: Cybersecurity, Saudi Arabia, cybercrimes, awareness;

1. Introduction

Saudi Arabia is one of the most advanced nations in the Middle East and the Arab world in using the latest technology [1]. Citizens and residents of Saudi Arabia are among the Internet's most significant users in the Arab world [2]. They are also among the first to use the latest technology tools and applications such as social media. Besides, it is one of the top countries to use modern technology like smartphones, mobile broadband, etc. [1]. It is evident in media that cyber-attacks are rising in both quantity and sophistication all over the world [3]. Internet users are negatively affected by cyber-attacks, resulting in emotional distress and leading people to stop using the Internet. Cybercrimes are among the very critical issues that face our society nowadays. We all have to be aware of these cyber crimes [4].

Cybercrime is a criminal activity using the Internet. These crimes are numerous, like virus infections, bank account theft, theft of personal information, identity theft, and hacking. It will be a major problem being a victim of any of these cybercrimes, especially for those who do not recognize criminal activities using technology [5] [6]. There is a vital requirement to raise awareness of cybercrimes, especially among those who lack the necessary experience to deal with the Internet and websites [7]. There is a necessity for launching cybersecurity awareness campaigns to provide Saudi Arabian users with useful information about cybercrimes. Besides, there must be campaigns to raise the level of awareness among internet users. These campaigns are considered the first line of defense for reducing cybercrimes. Moreover, these campaigns can provide employees, youth, students, and stakeholders with knowledge about interacting online safely.

There is a difference in meaning between the three common terms: awareness, training, and education [8]. Education is for security professionals to build in-depth knowledge; training provides employees with a proper level of skills to make them able to perform what they are asked to perform securely; as for awareness, it gives the employees information and informal training to raise their standard of awareness about security [9]. Most of Saudi Arabia's users of the Internet are young people. They lack the required awareness and knowledge to protect them from cybercrimes. In most cases, we find that the weakest part in cybersecurity is the human element while the number of online crimes is increasing. Cybersecurity awareness campaigns are necessary. Higher Education Information Security Council provides cybersecurity awareness campaigns and material to guide universities and educate them about security by publishing content on various topics such as privacy, passwords, and ransomware programs each October in National Cyber Security Awareness Month (NCSAM) [10]. Some countries like Australia, Canada, USA, and UK have made Cyber Security Awareness (CSA) campaigns to assist the local committees and strategies [11]. If we compare these countries with other countries in Africa such as South Africa, Kenya, and Mauritius that lack awareness and training [12]. The Saudis revealed a significant difference between their Internet usage and their knowledge of cybercrime threats. Non-awareness among youth has created a potential imbalance between safe internet usage and vulnerability against crime. Most people heard about cybercrimes but significantly less is aware of the associated legislation to combat these crimes [13]. Wealth is both a blessing and a curse [24]. The wealth of Saudi Arabia has made it a specific target for cybercriminals.

According to statistics published by Statista [25], Fig1 shows that Saudi Arabia is the country most exposed to extortion from ransomware. Most of the citizens of Saudi Arabia use the Internet at an exaggerated rate. Despite this, they do not have a good idea of cybersecurity awareness against the cybercrimes that they are likely to encounter when using the Internet. Therefore, awareness must be increased in cybersecurity. Cybersecurity awareness against cybercrimes plays an essential and crucial role in preventing and reducing cyber-attacks. The majority of internet users in Saudi society lack the appropriate practice of cybersecurity [23]. Therefore, the main objective of our paper is to analyze the pattern of cybersecurity awareness in Saudi Arabia and how to react to cybercrimes if they occur. This study was conducted on Jouf University students to identify cybersecurity awareness against cybercrimes and the risks associated with them in Saudi society. By understanding the role of applying cybersecurity procedures and compliance with education and training programs to eliminate these cybercrimes.

The rest of this paper is organized as follows: In section 2, we present an overview of previous literature related to security awareness against cybercrime. In section 3, we explain the conducted survey study to explore the extent of Saudi society's understanding of cybercrimes; this study has been applied to Jouf University students in various colleges who do not have a comprehensive knowledge of using technology and dealing with its applications. Then, we discuss our results and findings in section 4. Finally, we present the conclusion of our work by developing a framework for enhancing cybersecurity awareness in Saudi Arabia.

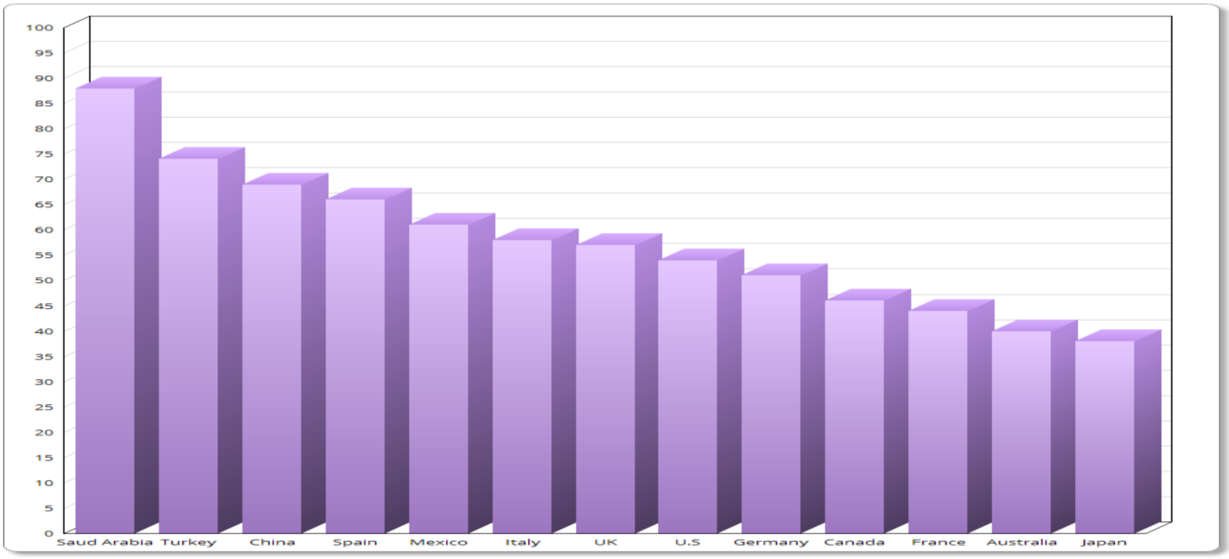

Fig.1 . Saudi Arabia hardest hit by Ransomware.

2. Literature review

Cybersecurity is a crucial topic; several research efforts have been done to investigate emerging cybersecurity issues. This research field is one of the most evolving and developing fields, however, it requires further work. One of the most industrialized nations, Saudi Arabia, has embraced new technologies and the Internet. However, this rapid development may lead to negative consequences for the country's residents because they are not fully aware of the cybercrimes associated with technology. Many people do not know about cyber attacks or how to deal with them. This study [22] concluded that most participants prefer having an application to guide them with the information required for security awareness.

A study [14] showed that Saudi Arabia was considered as one of the highest affected countries to be a cybercrime victim. Moreover, cybercrime is increasing across Saudi Arabia because the Internet offered an excellent chance to cybercriminals in facilitating their crimes. This research discussed the situation of Saudi Arabian authorities against cybercrime. The paper addressed cybercrime in Saudi Arabia, and it also discussed the anti-cybercrime law to face this phenomenon. The researcher focused on cybercrime in Saudi Arabia and internet users in the Kingdom. The Saudis revealed a significant difference between their Internet usage and their knowledge of cybercrime threats. The study found that 40 % of adults and youth in the Kingdom do not know that malware works discreetly, making it easy for users to know if a computer is compromised. Besides, more than half, about (55 %), are not sure if their computers are clean and free of viruses or any other harmful applications. After that, the researchers discussed the Cyber laws that already exist in Saudi Arabia and conclude that although the cybercrimes law exist since 2007, there is not enough youth awareness. It made an imbalance between using the Internet safely and vulnerability towards crimes. The study showed that most people know about cybercrime but lackingawareness to these cyber crimes' threats [13].

Another study [15] explained that students at a higher level of education know the security of smartphones. Still, , they do not have enough awareness of the safety dangers, risks, or necessary security practices. Authors recommended practice, training, and awareness campaigns. The study for [16] found that most college students in the United States of America did not participate in information security awareness to give them more information about cybercrimes. However, they recognized the urgent need and the importance of -cybersecurity training . Kim illustrated another finding of his study, which emphasize that the students' security learning should be implemented gradually. To improve their specific behavior, they need to focus on both information security and awareness training. Hence, it is clear that there had to be information security and awareness training.

A study by [17] discussed the relationship between internet users' possibility of falling victim to phishing. Phishing is a kind of social engineering that uses emails to get personal and critical information from computers; it can lead to many dangerous problems related to safety, such as falling victim to blackmail. Paper [18] argued that cybercrime awareness is affected by gender, age, and knowledge. A study found that female students are more aware than male students of cybercrime. As for the age group, students between 23-25 years are more aware of cybercrime perception than those between 18-19 years. Students in the age group between 24-25 and more than 25 years have enough cybercrime awareness compared to 18-23 years. This study recommends training or educating young people with some information and knowledge on cybercrime and cybersecurity. This study could help increase their standard of awareness to protect them from cybercrime.

Paper [19] revealed that there is an apparent lack of knowledge of information security concepts. Moreover, the results show an evident lack of understanding of information security, security images, and deficient awareness levels. It provided an overall view of the level of information security awareness in the academic environment. The paper states that security start with everyone's awareness. Besides, if the participants' awareness increases, it would result in increased network security. It also would result in personal and organizational protection and not be a victim of cybercrimes and hacking. According to Kaspersky's lab, another study [20] showed that Saudi Arabia had the ninth highest county of Information Security attacks globally in 2008 and the seventh highest in 2009 and twelfth in 2010. They argued that Poor information security in countries like Saudi Arabia resulted in increasing cybercrimes and viruses. It created what is known as "easy targets" for Denial of Service attacks against businesses worldwide. It is necessary to understand the reasons for some countries like China, Russia, and Saudi Arabia have been a target for cybercrimes with high levels of attacks. This study suggested that such a level of aggression can result from a lack of Information Security Awareness among the Saudi people. This paper also suggested that the lack of information security awareness may be due to Saudi culture's tribal nature. A survey of 462 Saudis indicates that information security awareness is, in fact, very low and related to several information security risks to Saudi culture.

Paper [21] discussed the need for security awareness in various academic fields in the Middle East.

This study was accomplished by presenting the results of numerous security awareness studies conducted among students and professionals in the educational sector despite offering little insight into how to deal better with training to eliminate security risks. It also he discussed that information security awareness, education, and training are extremely important. They have been part of an organization's overall security management and risk assessment plans for every class of administrators and users to minimize the risk of cyber-attacks.

In study [22]; this paper discussed the cybersecurity awareness of Saudi Arabia people through different contexts. They offered a quantitative online survey to collect data and information concerning cybersecurity awareness in the Kingdom of Saudi Arabia. The study found that the participants' understanding of cyber-crime threats, cybersecurity activities, and both government and organizations' role in ensuring information safe while using the Internet is minimal. However, they had a good knowledge of IT. The majority expressed their desire to have an application based model to create cybersecurity awareness in the region. The results referred to a rise in the number of cybercrimes in the Kingdom of Saudi Arabia, but there is no particular approach followed to increase cybersecurity awareness among the people in the region except CERT regulations and online information on government websites. The study found a severe need to develop a model to create cybersecurity awareness to face cybercrime.

Another study in the Al-Namas region conducted a test and assessed cybercrime risk and awareness about these crimes. This study shed light on people who have an excellent knowledge of using applications. The study focused on knowing the leading causes of these cybercrimes, as it inferred that the outputs behind these crimes are: nationality, financial, political, and cultural. There was a marked lack of awareness in the knowledge of cybercrime [23].

This paper aims to understand the pattern of how young Saudi especially those who do not have complete knowledge of using the technology deal with cybercrime and to understand the effect of conforming to the training and courses in cybersecurity to give more understanding and insights required to meet the requirements of cybersecurity and cybercrimes awareness.

3. Methodology

Cybersecurity is a main concern in the current time. However, it did not receive enough attention in terms of awareness and training. Most people deal with cybercrime based on being not real crimes. A quantitative approach is considered appropriate to conduct our study and explain a particular phenomenon of awareness about cybersecurity and cybercrime in a specific region.

Our study aims to find out the answer to the research questions concerning awareness of cybersecurity through numerical evidence. We used this research method to analyze the data collected through the survey and statistical results [27] [28]. The quantitative methodology offers an effective way of understanding the phenomena being studied by gathering numerical data and generalizing it across groups, which in this research are students at Jouf University. This approach will help to understand the pattern of awareness level of specific age groups and the extent of their knowledge of applying acceptable cybersecurity practices and how to deal with cybercrimes.

The sampling method used was nonrandomized and straightforward; 379 male and female students were chosen from different courses and education levels at Jouf University. Data was collected by a survey, which includes two sections in addition to demographic factors. The first section discusses the application of the best personal cybersecurity practices, while the second section discussed cybercrimes and local cybercrimes law. SPSS software and correlation coefficient were used for analyzing data.

Governments, institutions, and individuals in the world in general and Saudi Arabia, in particular, are widely using Internet technology, which makes users vulnerable to cybercrimes at any time [29]. Saudi Arabia has a significant cybersecurity trend through the National Cybersecurity Authority based on its missions as the competent authority in Saudi Arabia in cybersecurity [26]. Saudi Arabia focuses to enhance cybersecurity by collaborating with industries, to achieve development in cybersecurity, and teaching security standards to employees and people. Despite the expansion of Saudi efforts, there is still an urgent need for training and cybersecurity education. Therefore, the objective reflected in this study is to measure users' awareness and explore participants' experiences and attitudes.

The survey was used and intended to target university students; being citizens over 18, adults using technology. 22.7% of the study sample were male, compared to 77.3% of the female participants, who are the largest group in the study sample. Since this study aims to study the pattern of awareness in cybersecurity and cybercrimes, the target audience members questioned the following points:

- What is the extent of general knowledge of cybersecurity concepts?
- Does the public often apply different protection methods and techniques or not?
- What are the ways of dealing with cybercrimes, if any?
- Are Saudi government apps being used that respond to reporters related to cybercrimes?
- What are the perceptions about the regulations of the local laws related to cybercrime?
- What is the focus of training courses in cybersecurity and cybercrimes?
- What are the perceptions about enriching content and guiding Saudi society on how to deal with cybercrimes?

  The survey was published in October 2020. 379 completed responses were received during the study week.

4. Findings And Discussion

Cybersecurity awareness is the level of understanding of the internet users about the best practices of cybersecurity. People have varying levels of security awareness. There was a noticeable increase in participants who had the right information (or little information) about cybersecurity concepts, where their percentage was 73.6%. While 26.4% of the study sample do not have a minimum level of knowledge about cybersecurity. It is considered a large percentage compared to the efforts made by Saudi Arabia to raise awareness of cybersecurity as it is one of the leading countries in the field of cybersecurity. Saudi Arabia focuses on strengthening the cybercrime Law, and cybersecurity Systems. The lack of awareness is due to a set of potential factors, the most compelling of which is because this sample is ignorant of the threats that can be posed by these cybercrimes and do not realize the value of knowledge of cybersecurity. It is worth noting that 3 out of 21 participants exposed to cybercrime do not have any information about cybersecurity and cybercrime, so they did not know what the procedures to respond. Only one participant dealt with the crime correctly and informed relevant authorities through a mobile application that respond to cybercrime reports. Another interesting finding which may create the main concern, 10.6% of respondents do not know whether their smart devices have been subjected to cybercrimes or not, and this is due to the negligence of the nature of malware and the means of penetration [13].

The survey results indicate that most of the participants' who applied correct cybersecurity practices had an interest in training courses related to cybersecurity and cybercrimes awareness. In addition to the use of cybercrimes protection techniques, more cybercrime knowledge and awareness would keep cybercrimes at the lowest level possible. There is strong evidence indicating that cybersecurity awareness training is the main reason for increasing cybersecurity effectiveness [29]. Training and education are the best way to empower Internet users to reduce cybercrimes. Despite this, 82.1% of the total study sample, which is the largest percentage, did not receive any training or educational content for cybersecurity cybercrime. Our research can support the study results [18] the awareness rate of female students in cybersecurity and cybercrime is more than that of male students. Fig 2 shows the pattern of whether or not optimal cybersecurity practices are applied in the participants' devices.

Also, it is noticeable that there is a lack of interest in knowing local regulations and cybercrimes laws. However, there has been an increase in fraud attempts, with 63.9% of respondents experiencing a fraud attempt through unnatural links, fake emails, or social engineering. However, these indents of fraud were ignored without reporting to authorities. This study indicates that many people still do not consider cybercrime as a real threat that must be reported.

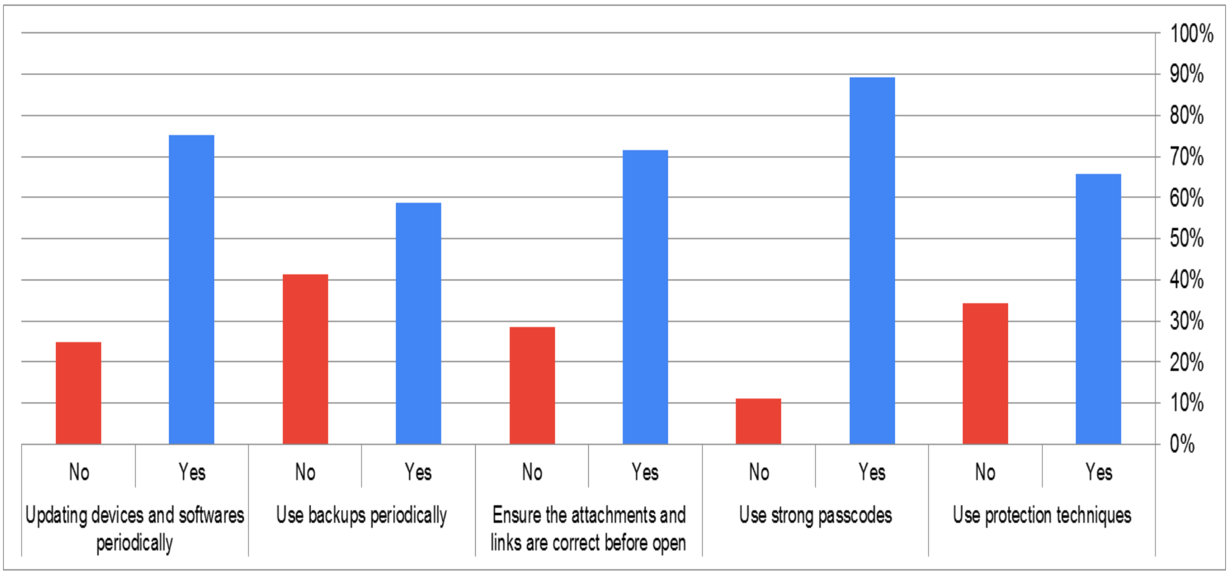

Fig. 2. Percentages of usingn cybersecurity practices (n=379) .

The local laws and regulations to combat cybercrime in Saudi Arabia cover cybercrimes and its penalties. The survey results have shown that more than half of the study sample does not know local cybercrime laws, so there is an urgent need to shed light on these laws, strengthen them, and publish them. Training and education courses should be appropriate with the local cybercrime law to expand knowledge of these laws to the maximum extent. The participants have been questioned whether they preferred to enrich the public digital content about cybersecurity and cybercrime, 96.6% of internet users believed that they need more awareness and education in this area.

In general, the results indicate that despite the increasing interest in awareness and education in cybersecurity and cybercrime, but there are still some individuals who need to lift the level of awareness, especially about dealing with and reporting cybercrimes. The results of this study summarized that the common points between participants for whom cybercrimes occurred due to several possible reasons could be listed as follows:

- Not knowing the seriousness of cybercrimes.
- Poor use of optimal cybersecurity practices.
- Lack of attention to awareness in cybersecurity and cybercrime
- The training courses are not compatible with cybersecurity precautions and cybercrimes.
- Failure to report cybercrime in the belief that it is not considered as a crime with punishment.

Although many Saudi efforts are included in cybersecurity training and awareness, there is still an urgent need to develop many flexible and interactive frameworks, methods, and tools to enrich cybersecurity content and deal with cybercrime in Saudi Arabia.

Fig 3 presents the framework to increase the effectiveness of cybersecurity awareness and reduce cyber-crimes in Saudi Arabia. To counter cyberattacks, internet users need a thorough knowledge of security, in general, to help them remain more secure on the Internet. Owing to the dependency of anything surrounding us on the Internet, cybersecurity has been more daunting than ever because internet users are in danger at any moment. Internet users need to have humble knowledge of the essentials of cybersecurity to work properly with diverse devices and technology and to apply the optimal practices of cybersecurity to maintain high levels of cybersecurity.

Training and cybersecurity awareness are not adequate immunity to cyber attacks. Rather they are a procedure for addressing these cybercrimes, as devices may be faced by these cybercrimes. Therefore to mitigate the potential harm, one must understand the nature of these cybercrimes and how to deal with them as much as possible. In addition to knowing the local laws in Saudi Arabia against cybercrimes to deal with these crimes as necessary and informing the responsible authorities to limit the spread of such crimes.

There is an immediate need for more attempts to post, in compliance with local legislation and policy on these crimes, content relevant to dealing with these cybercrimes. Finally, the experience gained and education can make a big difference in finding a high level of awareness in the field of cybersecurity and reducing cybercrimes.

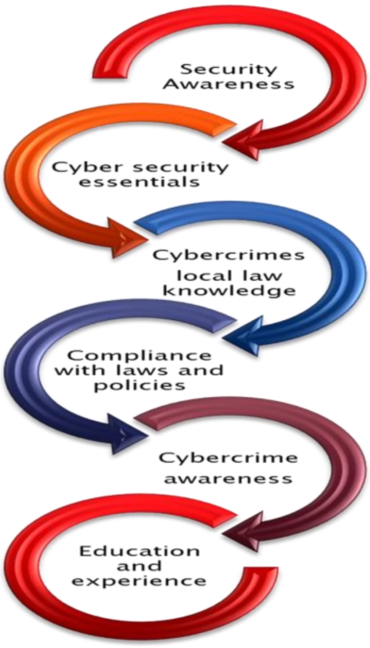
Security Awareness
Cyber security essentials
Cybercrimes local law knowledge
Compliance with laws and policies
Cybercrime awareness
Education and experience

Fig. 3. Cybersecurity awareness framework.

5. Conclusion

This paper aims to study the pattern of awareness of cybersecurity and cyber-crime in Saudi Arabia by the case study of Jouf University students to understand the current situation of cybersecurity awareness better. The analysis was applied by testing through two parts: (1) using optimal cybersecurity practices, (2) cyber crimes, reporting, and legal procedures in Saudi Arabia. Our results indicate that although there is an increase in awareness of cybersecurity by the participants, there is an urgent need to understand cybersecurity and cybercrimes by training and education. They are the most powerful way to enable people to deal with cybercrime. The survey analysis results showed that most participants who faced cybercrimes did not deal with them according to the local legislation law, where the majority require extensive awareness programs to fill this gap. The study presented some factors that may increase cybercrime by extrapolating the relationship between cybersecurity awareness and dealing with cybercrimes faced by participants. We developed a framework that helps internet users with the ability to reduce cybercrime. This study's most apparent result is that most participants need more education and content enrichment with cybercrime and how to deal with it according to local legislation in Saudi Arabia. Undoubtedly, there is still a need for more research and investigation in cybersecurity awareness. It is considered an emerging field of study to increase the level of understanding of Saudi society.

References

[1] Al-Saggaf Y, Weckert J. Privacy from a Saudi Arabian Perspective. Journal of Information Ethics. 2011;20(1):34-53.
[2] Humayun, M., Jhanjhi, N., Alruwaili, M., Amalathas, S. S., Balasubramanian, V., & Selvaraj, B. (2020). Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things. IEEE Access, 8, 183665-183677.
[3]Symantec. 2013 Norton report: Cost per cybercrime victim up 50 percent. Retrieved from 0http://www.symantec.com/en/za/about/news/release/article.jsp?prid=20131029_01. 2013.
[4] Sukhai N. Hacking and cybercrime. New York, NY: ACM Press 2004.
[5] Asokhia MO. Enhancing National Development and Growth through Combating Cyber- crime/Internet Fraud: A Comparative Approach. Journal of Social Sciences. 2010;23(1):13-19.
[6] Mensch, Wilkie. Information security activities of college students: An exploratory study.Journal of Management Information and Decision Sciences. 2011.
[7] Wang HS, Chou CH, Tsai SN. A preliminary study of internet security education implied in a movie based English class in Taiwan's private vocational continuation high school. CNTE2008. 2008.
[8] Ahmad A, Maynard S. Teaching information security management: reflections and experiences. Information Management & Computer Security. 2014;22(5):513-536.
[9] Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1.
[11] Leuprecht C, Maclellan S. Governing Cyber Security in Canada, Australia, and the United States. Carol Bonnett. .
[12] Doyle K. SA security policy trails Africa. ITWeb. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=143303. 2015.

[13] Elnaim BM. Cyber Crime in the Kingdom of Saudi Arabia: The Threat Today and the Expected Future. Information and Knowledge Management. 2013; 3:14-18.

[14] 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, 1-19.

Table 3. Summary of awareness of cybercrimes and local low cybersecurity practices. (n=379)

[15] Pramod D, Raman R. A study on user perception and awareness of smartphone security. Inter- national Journal of Applied Engineering Research. 2014;9(23):19133-19144.

[16] Kim. College students' use of social media for health in the USA and Korea. Information Research: An International Electronic Journal. 2014;19(4).

[17] Humayun, Mamoona, N. Z. Jhanjhi, Ahmed Alsayat, and Vasaki Ponnusamy. "Internet of things and ransomware: Evolution, mitigation and prevention." Egyptian Informatics Journal (2020).

[18] Rahman A, Hilwani A, Omar. Awareness of Young Internet Users towards Cybercrime: Evidence from Malysia. 2015.

[19] Al-Janabi . Al-Shourbaji A Study of Cyber Security Awareness in Educational Environment in the Middle East. Information & Knowledge Management. 2016;15(1).

[20] Alarifi A, Tootell H, Hyland P. Information Security Awareness in Saudi Arabia .2012.

[21] Aloul FA. The Need for Effective Information Security Awareness. Journal of Advances in In- formation Technology. 2012;3(3).

[22] Alotaibi F, Furnell S, Stengel I, Papadaki M. A survey of cyber-security awareness in Saudi Arabia. in 11th International Conference for Internet Technology and Secured Transactions (ICITST):154-158 2016.

[23] Zayid EIM, Farah NAA. A study on cybercrime awareness test in Saudi Arabia - Alnamas region. in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC):199-202 2017.

[24] Alqurashi RK. Cyber Attacks and Impacts: A Case Study in Saudi Arabia. International Jour- nal of Advanced Trends in Computer Science and Engineering. 2020;9(1):217-224.

[25] Feldman S. Saudi Arabia Hardest Hit by Ransomware. Retrieved 10 November 2020, from https://www.statista.com/chart/18028/ransomware-attacks-by-country .2020.

[26] Kok, S. H., A. Azween, and N. Z. Jhanjhi. "Evaluation metric for crypto-ransomware detection using machine learning." Journal of Information Security and Applications 55 (2020): 102646.

[27] Alferidah, Dhuha Khalid, and N. Z. Jhanjhi. "Cybersecurity Impact over Bigdata and IoT Growth." In 2020 International Conference on Computational Intelligence (ICCI), pp. 103-108. IEEE, 2020.

[28] Tugal-Tutkun I, Herbort CP. Laser flare photometry: a noninvasive, objective, and quantitative method to measure intraocular inflammation. International Ophthalmology. 2010;30(5):453-464.

[29] Muzafar, Saira, and N. Z. Jhanjhi. "Success Stories of ICT Implementation in Saudi Arabia." In Employing Recent Technologies for Improved Digital Governance, pp. 151-163. IGI Global, 2020.

Appendix

Table 1. Summary of respondents' demographic characteristics. (n=379)

Demographic Factor	**Characteristic**	**Count**	**Percentage**
Gender	Female	293	77.3
	Male	86	22.7
Age	18-20	211	55.7
	21-23	102	26.9
	26-24	44	11.6
	24 and more	22	6

Cybercrimes awarnesses	**Yes / No/ Might**	**Count**	**Percentage**
Cybercrimes occurs	Yes	21	5.5
	No	318	83.9
	Might	40	10.6
Dealing with government application related to cybercrime	Yes	80	21.1
	No	299	78.9
Review the local regulation related to cybercrimes	Yes	151	39.8
	No	85	22.4
	Might	143	37.7
Obtaining training course related to cybersecurity and cybercrime	Yes	68	17.9
	No	311	82.1
Suitability of training course with cybersecurity practices and local regulation related to cyber crime	Yes	134	35.4
	No	17	4.5
	Might	228	60.1
Support the enrichment of content on dealing with cybercrimes	Yes	366	96.6
	No	16	3.4

Cybersecurity Practices	**Yes / No/ Might**	**Count**	**Percentage**
Knowledge of cybersecurity concepts	Yes	74	19.5
	No	100	26.4
	Might	205	54.1
Use protection techniques	Yes	249	65.7
	No	130	26.9
Use strong passcode	Yes	339	89.4
	No	40	10.6
Ensure the attachments and links are correct before open	Yes	271	71.5
	No	108	29
Make Backup periodically	Yes	222	58.6
	No	157	41.4
Updating devices and software's periodically	Yes	285	75.2
	No	94	25