A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks

Gaseb Alotibi
Department of Computer and Information Technology, University of Tabuk, Saudi Arabia
galotaibi@ut.edu.sa (corresponding author)

Received: 22 February 2024 | Revised: 9 March 2024 | Accepted: 12 March 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.7123

ABSTRACT

Social engineering addresses a broad category of techniques aiming to persuade someone to reveal data or perform actions for criminal purposes, such as disclosing personal information about a particular target. Cybersecurity awareness is required to raise people's understanding of how these social engineering techniques are being used and so their capacity to exploit them. To accomplish this objective, primary focus is given to educating and training individuals on how to recognize such incidents and respond to them effectively. To protect people against social engineering threats, various cybersecurity models and approaches have been proposed. There are, however, a few differences between these models, since they are developed for specific purposes. Thus, the main objective of this study is to develop a cybersecurity awareness model specifically designed for Saudi students to protect them from social engineering attacks. The design science methodology was utilized in this study. The proposed model consists of four main stages: education and training, developing policies and guidelines, improving Saudi schools' security, as well as monitoring and evaluation. The model introduced can ensure the safety and privacy of students, teachers, and staff across different social platforms.

Keywords-cybersecurity; cybersecurity awareness; social media engineering; Saudi Arabia; design science

I. INTRODUCTION

Cybersecurity awareness refers in the enhancement of people's knowledge and comprehension of potential social engineering threats and risks [1]. As a form of attack in cybersecurity, social engineering involves exploiting human vulnerabilities by using influence, persuasion, deception, manipulation, and induction to breach cyberspace security. Cyberspace elements, such as infrastructure, data, resources, users, and operations must be secure in terms of confidentiality, integrity, availability, controllability, and auditability. The purpose of social engineering is to exploit human vulnerability to breach cyberspace security through social interactions [2, 3]. In the realm of cybersecurity, security awareness plays a crucial role in safeguarding individuals and organizations against potential security threats and risks. It empowers individuals to make informed decisions and take proactive measures to protect their digital assets. This paper discusses the concept of security awareness, its significance in the field of cybersecurity, and its impact on individuals and companies. Many organizations are automating their processes to offer their customers cheaper, faster, and easier ways to access their services due to the extensive developments in communication technology. During the last few years, the use of technology has increased exponentially, especially in the field of communications. Globally, over 7 billion people subscribe to mobile phones and more than 2 billion people use the Internet [4]. Approximately 294 billion emails and 5 billion mobile messages are exchanged every day [4, 5]. Technology deployment in developing countries, as well as its continued spread in developed countries, is expected to increase these numbers.

Globally, organizations are increasingly adopting automation as a means of delivering more efficient services. As technology has become a part of everyday life, many of their daily tasks are accomplished through mobile devices. These tasks include shopping, banking, and entertainment. All these services are managed by using communication technologies for effective information exchange. While these technologies are becoming increasingly employed, crimes connected with them also increase. Cybercrime is the process in which computer networks are utilized for the purpose of committing illegal acts [6]. Because most businesses and organizations rely more and more on communication technologies, it is of utmost importance that the information being exchanged is secure and unauthorized use is prevented.

Saudi Arabia has experienced a recent significant increase in the implementation of communication technologies, the Internet, and mobile technologies. This country is one of the fastest-developing countries in the Middle East. More than 18 million Internet users exist in the country, which means that approximately 66% of the population has access to the Internet, which equals to more than 18 million people. Among all, Facebook and X (Twitter), are the most deployed social media platforms [7]. Many people use the Internet to buy products online. The total amount of e-commerce sales in the country is about $520 million, with 39% of Internet users purchasing products online [8]. In the Kingdom of Saudi Arabia, there has been a boom in the utilization of smartphones while the penetration of the Internet is relatively new. Due to the lack of understanding and information about security measures that can be taken, it can be assumed that there is a lack of knowledge regarding cybersecurity. Literature mostly consists of studies conducted to assess cybersecurity awareness in developed Western countries. The Kingdom of Saudi Arabia, however, has a vastly different culture, social attitude, language, government regulations, and understanding of security importance.

Therefore, in this study, the realization of the students in Saudi schools when it comes to security awareness is discussed along with the security measures these students take to increase their security. Then, a comprehensive cybersecurity awareness model is developed for Saudi schools to effectively address security concerns related to the use of social media, adopting the design science approach. The model consists of four main stages: education and training of Saudi students, developing policies and guidelines, improving Saudi school security, and monitoring and evaluation. By addressing these areas, the model aims to create a safe and secure learning environment for students in Saudi schools.

The main contribution of the development of a cybersecurity awareness model for Saudi students is the establishment of a tailored approach which addresses specific cybersecurity challenges faced by Saudi students on a daily basis. With the assistance of this model, students can navigate the digital world with confidence and security as they enhance their digital literacy, promote responsible behavior, and contribute to the government's efforts to ensure cybersecurity in a national level. The model was created implementing the design science approach. It is a systematic and rigorous approach that could be adopted when developing models and solutions based on the principles of modeling and analysis [9]. The model can evolve and respond to threats and changes in the educational landscape, making it both robust and adaptable.

A. Related Work

This section provides a review of the related work focusing on cybersecurity awareness in Saudi Arabia. Due to the rise of cyberattacks in the developed world, monitoring cybercrimes has attracted a great deal of scientific attention. Several recent approaches of assessing cybercrime knowledge either globally or focused on the Saudi Arabian cybercrime scene are discussed below.

Authors in [10] examined the Saudi national level of cybersecurity awareness through a quantitative, online study employing 629 participants (70% males and 30% females). It was found that although the participants had adequate IT knowledge, they did not have a high level of awareness regarding cybercrime, cybersecurity practices, and their role in ensuring the integrity of information on the Internet and the safety of computers and data. Authors in [11] determined whether 116 employees working for governmental and private organizations in Riyadh were aware of phishing emails and how they should handle them. It was reported that they were mostly Saudi people who had not been employed in any companies working in the IT field. The survey indicated that the following data types were gathered: employee demographics, administrative specifics, employee understanding of the idea of email phishing, and employee awareness of the company's anti-phishing plan. The authors suggested that anti-phishing training programs should be put in place to raise awareness of the risks associated with phishing, given the low level of knowledge about this practice. Providing sufficient training to employees of an organization regarding email phishing is very important, as this is the most convenient approach to initiate these types of assaults.

Several studies have been conducted on the current risk of cybercrime in specific regions and the current level of awareness about these risks. In [12], 132 undergraduate students from Saudi Arabia's Alnamas district were surveyed regarding their knowledge of cybersecurity. According to the results, 69.6% of cybercrimes were committed via social media, with 57% of these crimes being sexual in nature, whereas 15% of the respondents had experienced cybercrime, and 80.7% wanted to receive training to improve their understanding regarding this matter. A survey of 633 Saudi public members was conducted in [13] in order to determine the level of information security knowledge. As part of the survey, respondents were asked about security awareness, password use, updates, data backups, and password management (changes and sharing). A total of 2325 people participated in the online survey administered in [14] that measured the level of information security awareness. The authors found that 35% of the participants were aware of general information security, 37% were aware of password security, 38% were aware of wireless network security, 40% were aware of social networking security, and 44% were aware of cloud storage security.

Measurements have been conducted on several aspects of awareness. Using three scenarios in terms of phishing email attacks, the authors in [15] attempted to determine the level of the awareness regarding phishing emails. The study employed embedded links, attachments, and social engineering to solicit sensitive information. Evaluations were made according to failure percentage, distribution by email types, and distribution by classes. The study found a failure rate of 80% for the embedded links and 40% for the attachments and requests of sensitive information. The authors reported that 38% of the embedded links, 50% of the attachments, and 46% of sensitive information failed to be delivered within the specified time frame for distribution by email. Finally, their study investigated several undergraduate students, from freshmen to seniors, from different levels of education. The authors reported that as many as 10% of all students had faced phishing attacks whereas as many as 70% of them students were victims.

By creating an online questionnaire and disseminating it among 161 individuals, authors in [16] explored whether conceptual or procedural knowledge had a positive effect on computer awareness. Positive results were found when both conceptual and procedural knowledge were applied to prevent further phishing attacks. Using the Technology Acceptance Model (TAM) as a basis for Open-Source Cloud Computing (OSCC), authors in [17] studied a model based on TAM in the Iraqi environment in order to determine possible improvements of organization awareness. A total of 385 participants were included in the study, and 500 questions were asked during a period of 5 months during which the survey was conducted. According to the results, OSCC adoption relies upon mediation between perception and intention, between perception and goals, and between attitude and goals. Authors in [18], using a quantitative questionnaire divided into structured and unstructured questions, investigated the level of Information Security Awareness (ISA) in Greek Information Technology students. It was a two-month-long study with 87 participants. According to the results, a good level of awareness was associated with a good level of behavioral patterns, and the relationship between the level of awareness and behavioral patterns was studied. To examine whether cloud computing will be accepted by Malaysian university students, authors in [19] selected 45 students from Malaysian universities and scored them on at least 150 questions regarding readiness, perception, knowledge, and security awareness. The purposes of the study were to measure the level of security awareness and to obtain general knowledge about cloud computing. The findings confirmed the lack of awareness concerning the latter.

To investigate the cognitive use of cloud computing in the educational environment, authors in [20] used the Theory of Planned Behavior (TPB) in conjunction with the Theory of Knowledge Creation (TKC). A total of 240 people participated in that study, with a response rate of 91.95%. The study focused on attitudes and perceptions of cloud computing, privacy and security perceptions, behavioral control understanding, and final goals associated with the employment of cloud computing. The researchers deployed one-sample statistics, one-sample Kolmogorov-Smirnov tests [21] and linear interpolation to assess the experiment outcomes. In [22], the authors looked into various ways to spread information security knowledge within a business, such as interactive films, internal training sessions, screen savers, email, and social media, with the goal of enhancing end-user behavior and awareness in the context of phishing attempts.

Various studies have been reported that investigate and recognize cybercrime [22, 31-40], data cracks [23, 41-50], and other digital risks [24, 25, 41-58].

II. METHODOLOGY

A comprehensive cybersecurity awareness model for Saudi schools is developed in this study using the design science approach. Generally, design science is known as a systematic and rigorous approach. It aids in creating models and solutions that incorporate modeling and analysis [9, 60, 61]. It is a powerful research methodology that combines theory and practice to create and evaluate innovative artifacts or systems [62]. By associating problem definition, design, evaluation, and implementation, researchers can address real-world challenges and contribute to technological advancements. Therefore, the method adopted in this paper comprised the following five steps, as shown in Figure 1.

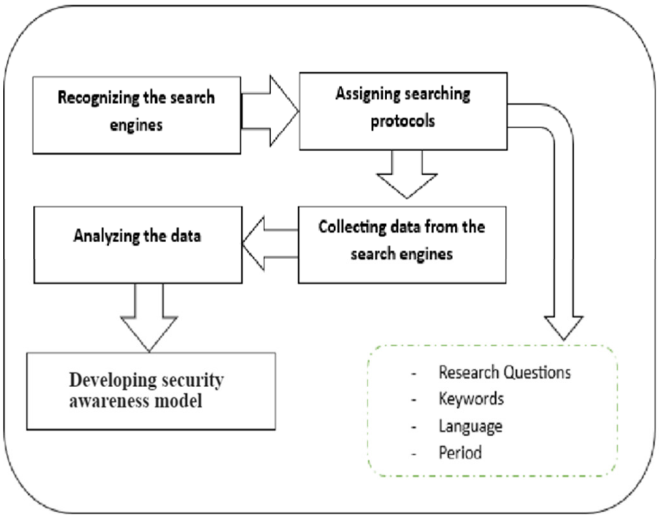
Recognizing the search engines
Assigning searching protocols
Analyzing the data
Collecting data from the search engines
Developing security awareness model
- Research Questions
- Keywords
- Language
- Period

Fig. 1. Development process

1) Recognizing Search Engines

In this step, popular search engines, i.e., IEEE Xplore, Web of Science, Scopus, Springer, and Google Scholar were identified. Each engine offers unique features and sources that scholars can use to locate relevant academic literature and scholarly articles.

2) Assigning Search Protocols

Search protocols to identify articles relevant to our study were defined. The protocols that must be adhered to for the survey to be successful include questions, keywords, the language of the survey, and time constraints. To collect valuable information about topics related to cybersecurity, security awareness, and Saudi schools, the protocols presented below were followed. First, the following research questions were developed to ensure that the search will be focused and targeted:

- How can cybersecurity awareness be effectively promoted in Saudi schools?
- What are the benefits of developing a cybersecurity model for protecting Saudi school students against social engineering on social media?

3) Data Collection from the Search Engines

This step involved gathering data from the search engines based on the search protocols defined above. The data collected from the search engines are displayed in Table I. A total of 9 articles were extracted from Scopus, 8 from IEEE Xplore, 12 from Web of Science, 2,163 from Springer Link, and 1,200 from Google Scholar. Table I and Figure 2 exhibit the results of the search.

4) Analyzing Data

In this stage, an analysis was conducted on the 3392 papers that were retrieved from the search engines. This study was performed to make sure the data utilized for the research were correct and relevant, and to exclude any irrelevant sources. Books, articles, book chapters, and reports that were judged as non-relevant to the research, were not considered. This rigorous selection procedure was carried out with the intention of excluding sources that would have biased findings and failed to advance the goals of the study. In this way, only relevant and reliable sources would be implemented. Using only the most relevant data enhances the credibility and validity of the research results. Consequently, 50 articles relating to Saudi Arabia's cybersecurity awareness are the final considered data set of this study.

TABLE I. PAPERS COLLECTED

Search engines	Keywords	Time	Totals

Scopus	"Cybersecurity";
	"Security awareness";
	"Saudi Arabia"
		2010-2024	200

IEEE Explorer			250
Web of Science			199
Springer Link			2163
Google Scholar			1200

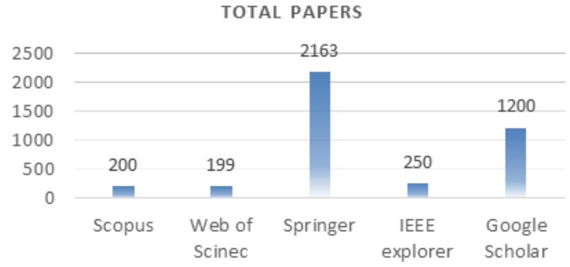

Fig. 2. Data collected from the search engines.

5) *Developing a Security Awareness Model*

This step involves developing a cybersecurity awareness model in relation to the use of social engineering on social media as a means of promoting cybersecurity knowledge in Saudi schools. After analyzing the 50 considered studies, 4 stages were identified to constitute the developed model (Figure 3):

a) *Education and Training of Saudi Students*

The purpose of this stage is to provide students, teachers, and other school staff with mandatory information and services to recognize potential risks associated with the usage of social media engineering. Three main tasks should be accomplished during this stage:

- **Adjusting Privacy Settings**: User privacy settings play a key role in safeguarding personal information. For students and teachers in Saudi Arabia to be protected against the misuses of social media platforms and online applications, privacy settings on these platforms and applications should be adjusted. Their understanding of what information is public and what information can be shared selectively with the public is critical. Furthermore, they should be informed about the consequences of sharing personal information, such as their telephone numbers and addresses, with third parties.
- **Safe Behavior**: Saudi children should be taught how to carefully surf on the Internet. Many precautions may be necessary to protect one's privacy, but among the most important measures and tips that people should take notice are: not to share private information with anyone outside their network, to stay away from suspicious connections/links, and to be careful while linking with unfamiliar people on social media. Furthermore, individuals should make sure that their passwords are strong, and they should be fully aware of any phishing attempts.
- **Threat Identification and Response:** Students and teachers in Saudi Arabia should be educated about scams and how to avoid them. It is important to teach them the risks associated with disclosing private information to unfamiliar people, as well as how to identify unnecessary texts that demand personal or private details. In addition, helpful information should also include ways to recognize suspect behavior and potential risks on websites and to distinguish the real from the fake ones.

b) *Developing Policies and Guidelines*

During this stage, there will be policies and guidelines that can assist possible threat evaluation.

- **Establishing Acceptable Use Policies**: Students and teachers at Saudi schools are being taught, through this course, how to use social networking tools for their schoolwork. To ensure acceptable usage, clear guidelines must be established. These policies should cover a wide range of topics, including:
  - Purpose: By highlighting the learning value of the social networking tools, the policymakers should distinctly state the intention of those tools.
  - Content: It is recommended that the use of social media tools as well as the content that is generated through them be outlined in guidelines that define what types of content are acceptable and appropriate for utilization.
  - Usage Limitations: Appropriate guidelines and policies must be identified and established to identify the constraints that can be imposed on social networking tools to make them effective and efficient.
  - Safety Measures: Several factors contribute to the preservation of private information online, including the recording of any suspicious activities, highlighting the value of online protection, and ensuring that personal details are protected.
  - Intellectual Property: As guidelines and policies are created, they should emphasize the importance for customers of social media tools to see the value in protecting their intellectual rights.
  - Consequences: It is crucial for students to be aware that non-compliance can lead to disciplinary actions, loss of privileges, and expulsion.
- **Outlining Consequences for Misuse**: Creating applicable management procedures for social engineering tools is significant, as is identifying the abuses that will be imposed on those who harm them maliciously. Such consequences to further encourage liable tool use and deter improper action.

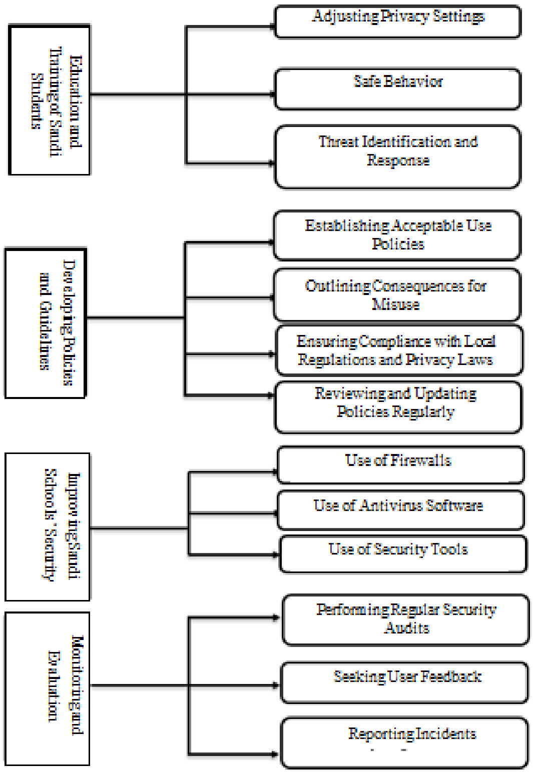
Education and Training of Saudi Students
Adjusting Privacy Settings
Safe Behavior
Threat Identification and Response
Developing Policies and Guidelines
Establishing Acceptable Use Policies
Outlining Consequences for Misuse
Ensuring Compliance with Local Regulations and Privacy Laws
Reviewing and Updating Policies Regularly
Improving Saudi Schools' Security
Use of Firewalls
Use of Antivirus Software
Use of Security Tools
Monitoring and Evaluation
Performing Regular Security Audits
Seeking User Feedback
Reporting Incidents

Fig. 3. Schematic of the developed cybersecurity awareness model.

- **Ensuring Compliance with Local Regulations and Privacy Laws**: Ensuring compliance with local rules and privacy laws is crucial when formulating guidelines and policies pertaining to the usage of social engineering media in Saudi schools. Schools are forced to follow the laws that regulate the former by creating school regulations. There are four tasks in this step:
    - Compliance Training: This teacher and staff training program includes a thorough education on social engineering tools. It helps individuals comprehend pertinent privacy regulations and guidelines, as well as how to apply them.
    - Data Protection Measures: Encrypting all data communicated when using social media is one of the many strong security methods that may be adopted to protect sensitive information, such as student grades, personal details, etc.
    - Regular Audits: By routinely examining and evaluating security and privacy policies, we can make sure that they are in accordance with local privacy and security requirements. Schools should carry out these audits to make sure that all local laws, rules, policies, and guidelines are followed.
    - Data Breach Response Plan: When schools expose sensitive data, unauthorized parties may gain access to sensitive information. Consequently, schools need to prepare a plan of action if there is a breach concerning the personal data of their students.
- **Reviewing and Updating Policies Regularly**: To ensure the effectiveness of the policies and guidelines, it is important to regularly review and update them. This includes considering any new security concerns or emerging threats that may require adjustments to the guidelines. Constant review and updating ensures that the social media use policies, remain relevant, and address the changing needs of Saudi schools.

c) Improving Saudi Schools' Security

Expanding security methods, precisely targeting social engineering channels in Saudi schools, is the third stage of upgrading school security in the country. To accomplish this, it is essential to implement technical tools and security measures to reassure that potential threats can be controlled. This stage consists of three security measures.

- **Use of Firewalls**: Any network, including those utilized in schools, needs a firewall to be secure. Schools can prevent potential problems by configuring firewall rules and protocols to monitor and block all kinds of unauthorized network traffic. Students can prevent unauthorized access to their computers and malicious activities, such as hacking attempts, if they take such measures.
- **Use of Antivirus Software**: Anti-malware software can be employed as a complementary feature to the antivirus software to protect computers from malicious software (malware). It is recommended that school computer systems be frequently updated with antivirus software so that potential threats cannot access them through social engineering and that potential threats are obstructed from emerging via those means. Additionally, antivirus software delivers real-time protection against known and future threats that are likely to appear soon.
- **Use of Security Tools**: School administrators should be aware that, beyond firewalls and antivirus software, some other security tools, such as intrusion detection systems and intrusion prevention systems are available to make the school campuses safer. It is possible to detect and mitigate potential security breaches by implementing these tools, which will improve their overall security.

d) Monitoring and Evaluation

Ensuring the successful implementation of security measures and periodically evaluating the efficacy of the cybersecurity awareness model are the main objectives of this phase. There are three primary duties involved:

- **Performing Regular Security Audits**: Conducting routine security audits is essential to monitoring and assessment. A thorough examination of several factors, including social engineering technologies, is necessary to carry out security audits of schools in an efficient manner.
- **Seeking User Feedback**: If educators actively seek input from students and staff, they may be able to provide them with insightful comments about how their security awareness model is being implemented.

- **Reporting Incidents**: Schools should create strong incident reporting mechanisms as soon as they become aware of social media engineering and put them timely into place.

III. FINDINGS AND DISCUSION

This part addresses the study's findings, the efficacy of the created cybersecurity awareness model, and the resolution of the research issues. The preceding segment elucidated the principal phases of the cybersecurity awareness framework designed to safeguard Saudi schoolchildren against social engineering via social media. The model gives students the tools they need to navigate the digital world safely and responsibly by teaching them about privacy settings, cybersecurity best practices, risk awareness, and responsible digital citizenship. This program helps to create a more secure and safe online learning environment for Saudi Arabian students. Based on the study's findings, the established research questions are addressed below.

A. How can Sybersecurity Awareness be Effectively Promoted in Saudi Schools?

Security awareness is essential to ensuring the wellbeing and safety of Saudi school employees, teachers, and students. Here are some strategies Saudi schools can deploy to successfully raise students' awareness of security issues:

- **Comprehensive Security Policies**: To encourage security awareness and foster a culture of safety in schools, complete security policies must be developed, put into place, and strictly enforced. These policies should involve a wide range of security topics, including physical security measures, cyber security, emergency planning, and access control.
- **Security Training Programs**: Teachers and staff members will be better equipped to recognize possible threats and learn how to respond to them in a timely, effective, and professional manner if regular security training programs are implemented in schools and universities. These seminars ought to include several subjects, such as recognizing suspicious activities, reporting events, and adhering to emergency procedures.
- **Awareness Campaigns**: Launching awareness programs that can attract a lot of interest and attention is one way to promote security awareness in Saudi schools. There are numerous campaign formats available to emphasize the value of security precautions and inform pupils of possible hazards. Posters, pamphlets, and digital media content are examples of these campaigns' collateral.
- **Engaging External Experts**: Some students can interact with external experts by attending seminars or presentations, in addition to receiving insightful advice and useful knowledge from them. Examples of these experts include cybersecurity specialists and law enforcement officials. With these experts' contributions, the learning process will be improved and made more pertinent as they can offer examples and best practices that come from actual circumstances.
- **Parent Involvement**: To promote the efforts being made in this area, educators can encourage parents of students enrolled in Saudi schools to take part in security awareness seminars. Schools can utilize a variety of strategies, such as hosting parent workshops or providing them with instructional materials, to make sure that parents are aware of the security measures in place and can reinforce them at home as well.
- **Technology Integration**: Technology can significantly enhance school security awareness if it is used on a regular basis as part of a regular school security program. To protect an organization from security breaches, one should install surveillance cameras, implement access control systems, and employ cybersecurity software.

B. Advantages of the developed Cybersecurity Model

The advantages of the developed cybersecurity model for Saudi school students are:

- Improved online safety
- Awareness raising
- Enhanced digital literacy
- Developed critical thinking skills
- Established ethical online behaviors
- Preventing measures against cybercrime

A comparative analysis between the developed model and the existing models can be seen in Table II.

TABLE II. COMPARATIVE ANALYSIS BETWEEN THE DEVELOPED AND EXISTING MODELS

Existing models	**Proposed Model**			
	Educating and training of Saudi students	**Developing policies and guidelines**	**Improving Saudi schools' security**	**Monitoring and evaluating**
[10]	×	√	√	×
[11]	×	√	√	×
[12]	×	√	√	√
[13]	×	√	√	√
[14]	×	×	×	×
[15]	×	×	×	√
[16]	×	√	×	×
[17]	×	√	×	√
[18]	×	×	×	×
[19]	×	×	×	×
[20]	×	√	×	√
[21]	×	×	×	×
[22]	×	×	×	√

The developed cybersecurity awareness model is complete and covers a wider range of awareness security phases than the existing model. For example, authors in [10, 11] covered developing policies and guidelines, and the issue of improving Saudi schools' security, whereas authors in [12, 13] covered the following three phases: developing policies and guidelines, improving Saudi schools' security, and the monitoring and evaluation. The education and training of Saudi students were not covered by the existing models.

IV. CONCLUSION

A security awareness program enhances understanding and knowledge of potential security threats and risks, as well as the ability to mitigate them. One of its primary objectives is to educate and train individuals so that they can recognize and respond effectively to various cybersecurity threats that may occur, including phishing attacks, malware infections, and social engineering attempts that aim to manipulate users. Different approaches and models have been proposed to address the issue of security awareness in different fields. The purpose of this study was to develop a comprehensive cybersecurity awareness model for Saudi school students so that they can effectively address security concerns surrounding the use of social media. However, several security challenges need to be addressed because of the rapid growth of social media engineering. There is a need to guarantee the safety of students and educators. This study applied the design science approach to create a comprehensive cybersecurity awareness model. The developed model incorporated four stages: education and training of Saudi students, developing policies and guidelines, improving Saudi schools' security, and monitoring and evaluation. Several tasks and activities associated with each stage were defined. The developed model for Saudi school students will reassure the safety and privacy of students, teachers, and staff as well as it will promote responsible and secure online behavior. As far as is known, this one is the first study on the topic directly focused on Saudi Arabia. The implementation of the developed cybersecurity awareness model in Saudi schools is the aim of future work in order to evaluate its effectiveness.

REFERENCES

[1] A. Parsaei, "Awareness and Social Engineering-Based Cyberattacks," *International Journal of Reliability, Risk and Safety: Theory and Application*, vol. 7, no. 1, pp. 31–36, Feb. 2024, https://doi.org/10.22034/IJRRS.2024.7.1.4.

[2] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: a domain ontology and knowledge graph application examples," *Cybersecurity*, vol. 4, no. 1, Aug. 2021, Art. no. 31, https://doi.org/10.1186/s42400-021-00094-6.

[3] A. Alshammari, "A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11445–11450, Aug. 2023, https://doi.org/10.48084/etasr.6091.

[4] N. Sandjojo, M. Zuhriyanto, and I. W. W. Pradnyana, "The Effects of Fear of Cybercrime and Information Systems Security Policy on National Vigilance," in *International Conference on Informatics, Multimedia, Cyber and Information System*, Jakarta, Indonesia, Nov. 2020, pp. 195–200, https://doi.org/10.1109/ICIMCIS51567.2020.9354283.

[5] A. Cetrulo, A. Sbardella, and M. E. Virgillito, "Vanishing social classes? Facts and figures of the Italian labour market," *Journal of Evolutionary Economics*, vol. 33, no. 1, pp. 97–148, Jan. 2023, https://doi.org/10.1007/s00191-022-00793-4.

[6] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012, https://doi.org/10.1109/SURV.2011.122111.00145.

[7] M. Bardus, A. Keriabian, M. Elbejjani, and S. Al-Hajj, "Assessing eHealth literacy among internet users in Lebanon: A cross-sectional study," *Digital Health*, vol. 8, Jan. 2022, Art. no. 20552076221119336, https://doi.org/10.1177/20552076221119336.

[8] A. S. Alqahtani, "Factors Influencing the Adoption of E-commerce in Saudi Arabia: Study of Online Shopping," Ph.D. dissertation, Flinders University, Adelaide, South Australia, 2016.

[9] A. Al-Dhaqm, S. Razak, and S. H. Othman, "Model Derivation System to Manage Database Forensic Investigation Domain Knowledge," in *IEEE Conference on Application, Information and Network Security*, Langkawi, Malaysia, Nov. 2018, pp. 75–80, https://doi.org/10.1109/AINS.2018.8631468.

[10] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A survey of cyber-security awareness in Saudi Arabia," in *11th International Conference for Internet Technology and Secured Transactions*, Barcelona, Spain, Dec. 2016, pp. 154–158, https://doi.org/10.1109/ICITST.2016.7856687.

[11] N. Innab, H. Al-Rashoud, R. Al-Mahawes, and W. Al-Shehri, "Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh," in *21st Saudi Computer Society National Computer Conference*, Riyadh, Saudi Arabia, Apr. 2018, pp. 1–5, https://doi.org/10.1109/NCG.2018.8593144.

[12] E. I. M. Zayid and N. A. A. Farah, "A study on cybercrime awareness test in Saudi Arabia - Alnamas region," in *2nd International Conference on Anti-Cyber Crimes*, Abha, Saudi Arabia, Mar. 2017, pp. 199–202, https://doi.org/10.1109/Anti-Cybercrime.2017.7905290.

[13] A. Alarifi, H. Tootell, and P. Hyland, "A study of information security awareness and practices in Saudi Arabia," in *International Conference on Communications and Information Technology*, Hammamet, Tunisia, Jun. 2012, pp. 6–12, https://doi.org/10.1109/ICCITechnol.2012.6285845.

[14] A. Alzahrani and K. Alomar, "Information Security Issues and Threats in Saudi Arabia: A Research Survey," *International Journal of Computer Science Issues*, vol. 13, no. 6, pp. 129–135, Nov. 2016, https://doi.org/10.20943/01201606.129135.

[15] R. C. Dodge, C. Carver, and A. J. Ferguson, "Phishing for user security awareness," *Computers & Security*, vol. 26, no. 1, pp. 73–80, Feb. 2007, https://doi.org/10.1016/j.cose.2006.10.009.

[16] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304–312, Sep. 2014, https://doi.org/10.1016/j.chb.2014.05.046.

[17] H. A. Albaroodi, M. Abomaali, and S. Manickam, "Iraqi's Organizations Awareness to Prompt Open Source Cloud Computing (OSCC) in Their Service: A Study," in *International Conference on Advances in Cyber Security*, Penang, Malaysia, Dec. 2020, pp. 305–319, https://doi.org/10.1007/978-981-15-2693-0_22.

[18] A. P. Filippidis, C. S. Hilas, G. Filippidis, and A. Politis, "Information security awareness of greek higher education students — Preliminary findings," in *7th International Conference on Modern Circuits and Systems Technologies*, Thessaloniki, Greece, Dec. 2018, pp. 1–4, https://doi.org/10.1109/MOCAST.2018.8376578.

[19] S. S. Md Kassim, M. Salleh, and A. Zainal, "Cloud Computing: A General User's Perception and Security Awareness in Malaysian Polytechnic," in *Pattern Analysis, Intelligent Security and the Internet of Things*, A. Abraham, A. K. Muda, and Y.-H. Choo, Eds. New York, NY, USA: Springer, 2015, pp. 131–140.

[20] Z. Asadi, M. Abdekhoda, and H. Nadrian, "Cloud computing services adoption among higher education faculties: development of a standardized questionnaire," *Education and Information Technologies*, vol. 25, no. 1, pp. 175–191, Jan. 2020, https://doi.org/10.1007/s10639-019-09932-0.

[21] F. J. Massey Jr., "The Kolmogorov-Smirnov Test for Goodness of Fit," *Journal of the American Statistical Association*, vol. 46, no. 253, pp. 68–78, Mar. 1951, https://doi.org/10.1080/01621459.1951.10500769.

[22] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, Mar. 2014, https://doi.org/10.1080/0144929X.2012.708787.

[23] A. M. R. Al- Dhaqm, S. H. Othman, S. Abd Razak, and A. Ngadi, "Towards adapting metamodelling technique for database forensics investigation domain," in *International Symposium on Biometrics and Security Technologies*, Kuala Lumpur, Malaysia, Aug. 2014, pp. 322–327, https://doi.org/10.1109/ISBAST.2014.7013142.

[24] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R. Kebande, and S. Hajar Othman, "Face Validation of Database Forensic Investigation Metamodel," *Infrastructures*, vol. 6, no. 2, Feb. 2021, Art. no. 13, https://doi.org/10.3390/infrastructures6020013.

[25] S. Abd Razak, N. H. Mohd Nazari, and A. Al-Dhaqm, "Data Anonymization Using Pseudonym System to Preserve Data Privacy," *IEEE Access*, vol. 8, pp. 43256–43264, 2020, https://doi.org/10.1109/ACCESS.2020.2977117.

[26] A. Aldhaqm, S. A. Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual Investigation Process Model for Managing Database Forensic Investigation Knowledge," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 12, no. 4, pp. 386–394, Feb. 2016, https://doi.org/10.19026/rjaset.12.2377.

[27] M. Ngadi, R. Al-Dhaqm, and A. Mohammed, "Detection and prevention of malicious activities on RDBMS relational database management systems," *International Journal of Scientific & Engineering Research*, vol. 3, no. 9, pp. 1–10, Oct. 2012.

[28] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Extraction of Common Concepts for the Mobile Forensics Domain," in *International Conference of Reliable Information and Communication Technology*, Johor Bahru, Malaysia, Apr. 2017, pp. 141–154, https://doi.org/10.1007/978-3-319-59427-9_16.

[29] A. Ali, S. Razak, S. Othman, and M. Arafat, "Towards Adapting Metamodeling approach for the Mobile Forensics Investigation Domain," in *International Conference on Innovation in Science and Technology*, Kuala Lumpur, Malaysia, Apr. 2015, pp. 364–367.

[30] M. A. Saleh, S. Hajar Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common Investigation Process Model for Internet of Things Forensics," in *2nd International Conference on Smart Computing and Electronic Enterprise*, Cameron Highlands, Malaysia, Jun. 2021, pp. 84–89, https://doi.org/10.1109/ICSCEE50312.2021.9498045.

[31] B. Zawali, R. A. Ikuesan, V. R. Kebande, S. Furnell, and A. A-Dhaqm, "Realising a Push Button Modality for Video-Based Forensics," *Infrastructures*, vol. 6, no. 4, Apr. 2021, Art. no. 54, https://doi.org/10.3390/infrastructures6040054.

[32] A. Al-Dhaqm *et al.*, "Digital Forensics Subdomains: The State of the Art and Future Directions," *IEEE Access*, vol. 9, pp. 152476–152502, 2021, https://doi.org/10.1109/ACCESS.2021.3124262.

[33] A. Aldhaqm, S. A. Razak, and S. H. Othman, "CommonInvestigation Process Model for Database Forensic Investiga-tion Discipline," in *International Conference on Innovation in Science and Technology*, Kuala Lumpur, Malaysia, Apr. 2015, pp. 297–300.

[34] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field," *Computational Intelligence and Neuroscience*, vol. 2022, 2022, Art. no. 8002963, https://doi.org/10.1155/2022/8002963.

[35] F. M. Ghabban, I. M. Alfadli, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Comparative Analysis of Network Forensic Tools and Network Forensics Processes," in *2nd International Conference on Smart Computing and Electronic Enterprise*, Cameron Highlands, Malaysia, Jun. 2021, pp. 78–83, https://doi.org/10.1109/ICSCEE50312.2021.9498226.

[36] O. Ameerbakhsh, F. M. Ghabban, I. M. Alfadli, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Digital Forensics Domain and Metamodeling Development Approaches," in *2nd International Conference on Smart Computing and Electronic Enterprise*, Cameron Highlands, Malaysia, Jun. 2021, pp. 67–71, https://doi.org/10.1109/ICSCEE50312.2021.9497935.

[37] A. A. Alhussan, A. Al-Dhaqm, W. M. S. Yafooz, A.-H. M. Emara, S. Bin Abd Razak, and D. S. Khafaga, "A Unified Forensic Model Applicable to the Database Forensics Field," *Electronics*, vol. 11, no. 9, Jan. 2022, Art. no. 1347, https://doi.org/10.3390/electronics11091347.

[38] F. M. Alotaibi, A. Al-Dhaqm, Y. D. Al-Otaibi, and A. A. Alsewari, "A Comprehensive Collection and Analysis Model for the Drone Forensics Field," *Sensors*, vol. 22, no. 17, Jan. 2022, Art. no. 6486, https://doi.org/10.3390/s22176486.

[39] W. M. S. Yafooz, A. Al-Dhaqm, and A. Alsaeedi, "Detecting Kids Cyberbullying Using Transfer Learning Approach: Transformer Fine-Tuning Models," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 255–267.

[40] A. A. Alhussan, A. Al-Dhaqm, W. M. S. Yafooz, S. B. A. Razak, A.-H. M. Emara, and D. S. Khafaga, "Towards Development of a High Abstract Model for Drone Forensic Domain," *Electronics*, vol. 11, no. 8, Jan. 2022, Art. no. 1168, https://doi.org/10.3390/electronics11081168.

[41] I. M. Alfadli, F. M. Ghabban, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "CIPM: Common Identification Process Model for Database Forensics Field," in *2nd International Conference on Smart Computing and Electronic Enterprise*, Cameron Highlands, Malaysia, Jun. 2021, pp. 72–77, https://doi.org/10.1109/ICSCEE50312.2021.9498014.

[42] A. Al-Dhaqm, S. H. Othman, W. M. S. Yafooz, and A. Ali, "Review of Information Security Management Frameworks," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 69–80.

[43] M. Salem, S. H. Othman, A. Al-Dhaqm, and A. Ali, "Development of Metamodel for Information Security Risk Management," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 243–253.

[44] A. Al-Dhaqm, W. M. S. Yafooz, S. H. Othman, and A. Ali, "Database Forensics Field and Children Crimes," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 81–92.

[45] M. Saleh *et al.*, "A Metamodeling Approach for IoT Forensic Investigation," *Electronics*, vol. 12, no. 3, Jan. 2023, Art. no. 524, https://doi.org/10.3390/electronics12030524.

[46] A. Ali, S. A. Razak, S. H. Othman, R. R. Marie, A. Al-Dhaqm, and M. Nasser, "Validating Mobile Forensic Metamodel Using Tracing Method," in *Advances on Intelligent Informatics and Computing*, F. Saeed, F. Mohammed, and F. Ghaleb, Eds. New York, NY, USA: Springer, 2021, pp. 473–482.

[47] D. S. A. Baras, S. H. Othman, A. Al-Dhaqm, and R. Z. R. M. Radzi, "Information Security Management Metamodel (ISMM) Validation and Verification through Frequency-based Selection Technique," in *International Conference on Data Science and Its Applications*, Bandung, Indonesia, Oct. 2021, pp. 292–297, https://doi.org/10.1109/ICoDSA53588.2021.9617527.

[48] A. M. R. Al-Dhaqm, "Simplified Database Forensic Invetigation Using Metamodeling Approach," Ph.D. dissertation, University of Technology Malaysia, Johor, Malaysia, 2019.

[49] V. R. Kebande and I. Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)," in *4th International Conference on Future Internet of Things and Cloud*, Vienna, Austria, Aug. 2016, pp. 356–362, https://doi.org/10.1109/FiCloud.2016.57.

[50] V. Kebande and H. S. Venter, "Requirements for Achieving Digital Forensic Readiness in the Cloud Environment using an NMB Solution," in *11th International Conference on Cyber Warfare and Security*, Boston, MA, USA, Mar. 2016, pp. 1–9.

[51] V. R. Kebande and H. S. Venter, "A comparative analysis of digital forensic readiness models using CFRaaS as a baseline," *WIREs Forensic Science*, vol. 1, no. 6, 2019, Art. no. e1350, https://doi.org/10.1002/wfs2.1350.

[52] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," *IEEE Access*, vol. 8, pp. 173359–173375, 2020, https://doi.org/10.1109/ACCESS.2020.3014615.

[53] A. Al-Dhaqm *et al.*, "Categorization and Organization of Database Forensic Investigation Processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020, https://doi.org/10.1109/ACCESS.2020.3000747.

[54] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," *IEEE Access*, vol. 8, pp. 145018–145032, 2020, https://doi.org/10.1109/ACCESS.2020.3008696.

[55] V. R. Kebande, R. A. Ikuesan, N. M. Karie, S. Alawadi, K.-K. R. Choo, and A. Al-Dhaqm, "Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments," *Forensic Science International: Reports*, vol. 2, Dec. 2020, Art. no. 100122, https://doi.org/10.1016/j.fsir.2020.100122.

[56] V. R. Kebande, R. A. Ikuesan, and N. M. Karie, "Review of Blockchain Forensics Challenges," in *Blockchain Security in Cloud Computing*, K. M. Baalamurugan, S. R. Kumar, A. Kumar, V. Kumar, and S. Padmanaban, Eds. New York, NY, USA: Springer, 2022, pp. 33–50.

[57] V. R. Kebande and K.-K. R. Choo, "Finite state machine for cloud forensic readiness as a service (CFRaaS) events," *Security and Privacy*, vol. 5, no. 1, 2022, Art. no. e182, https://doi.org/10.1002/spy2.182.

[58] S. Makura, H. S. Venter, V. R. Kebande, N. M. Karie, R. A. Ikuesan, and S. Alawadi, "Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring," *Security and Privacy*, vol. 4, no. 3, 2021, Art. no. e149, https://doi.org/10.1002/spy2.149.

[59] V. R. Kebande, N. M. Karie, R. A. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," *WIREs Forensic Science*, vol. 2, no. 5, 2020, Art. no. e1372, https://doi.org/10.1002/wfs2.1372.

[60] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, https://doi.org/10.48084/etasr.6195.

[61] A. S. Alraddadi, "A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11505–11510, Aug. 2023, https://doi.org/10.48084/etasr.6128.

[62] A. Al-Dhaqm, W. M. S. Yafooz, S. H. Othman, and A. Ali, "Database Forensics Field and Children Crimes," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. New York, NY, USA: Springer, 2023, pp. 81–92.