Journal of Theoretical and Applied Information Technology
15th August 2022. Vol.100. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE IMPACT OF ENHANCING AWARENESS OF CYBERSECURITY ON UNIVERSITIES STUDENTS: A SURVEY PAPER

MARAM MOHAMMED[1], DOAA M. BAMASOUD[2]

[1]Master Student, Department of Information Systems, College of Computing and Information Technology, University of Bisha, Bisha, 61922, Saudi Arabia

[2]Assistant Professor, Department of Information Systems, College of Computing and Information Technology, University of Bisha, Bisha, 61922, Saudi Arabia

E-mail: [1]440804865@ub.edu.sa, [2]dbamasoud@ub.edu.sa

ABSTRACT

The great technological development and digital transformations that the world is witnessing increase the rate of cyber threats and cybercrime, and due to the Covid19 pandemic, education, and commerce have relied on the Internet for the continuation of education and to maintain the economy. Threats arising from the behaviors of the individuals are among the main cyber threats, this appears from the limited awareness of individuals about cyber security and its threats. This survey paper discusses the importance of enhancing cyber security awareness among university students in Saudi Arabia to reduce cyber threats. As cybersecurity awareness is one of the areas of cybersecurity controls that aim to enhance awareness of cybersecurity, its threats, and risks, and build a positive cybersecurity culture. In addition, cybersecurity awareness is an important component of ensuring the protection and privacy of critical information assets. Students' awareness of cybersecurity, its threats, and risks enhances students' references to action when facing cybercrime to protect the information, and technology assets to reach safe cyberspace to achieve the Saudi Arabia Vision of 2030.

Keywords: *Cyber Security Awareness, Cyber Threats, Enhance Cyber Security, Cyber Security, Higher Education Students*

1. INTRODUCTION

The great technological development and digital transformations that the world is witnessing increase the proportion of cyber threats and cybercrimes. Because of the Covid-19, total dependence on (distance education, e-government, e-commerce, and many others) has become on the Internet, this opens the way for a focus on enhancing cybersecurity awareness. Cybersecurity is defined as the process that includes several different processes in protecting basic software, processes, and technologies, data from damage, infection, or unauthorized access, people, and devices [1]. In addition, enhancing cyber security is one of the basic controls that have been published for cyber security controls by the National Cyber Security Authority, which consisted of several sub-controls, including (asset management, management of login identities and powers, mobile device security, e-mail protection, and others) [2]. The Saudi Minister of Trade and Investment, Dr. Majid bin Abdullah Al-Qasabi, confirmed in his speech in February 2020 that cyber threats in the region are increasing, and that the Kingdom is the most targeted, which requires double action to combat threats. However, organizations incur higher costs in handling cybersecurity incidents. The author in [3] said Saudi Arabia has tightened its cyber defenses, and the government has established a National Computer Emergency Response Team (CERT), which is responsible for raising public awareness of cybersecurity, responding to major incidents, and monitoring threats.

Tianfield [4] defined cybersecurity situational awareness (CSSA), awareness is an intelligence-based contextual understanding, situational awareness as the understanding of what is happening, how it has developed in recent times, and how it can go away in a short time. From a methodological point of view, the perception of the situation is achieved through the application of

appropriate mechanisms of assessment, evaluation, and inference, to generate an understanding of the situation. There has been a growing focus in recent years on the role of individual behavior in minimizing cyber risks. However, the understanding of how individuals differ in their cybersecurity awareness, knowledge, and behavior is still very limited, when faced with diverse cyber risks [5]. The author in [6] demonstrated that awareness of data privacy is one of the main problems related to data privacy. However, most college students are not aware of data privacy issues. Since it can reveal a lot of private data due to users' data breaches, and the potential for attackers to tamper with emails and deceive users onto a fake domain site where they can monitor users' passwords and logins, it is imperative to promote data privacy awareness of its importance. Most groups that use a network are university students, so they must be the most aware of cybersecurity, and at an early stage, a culture of cybersecurity awareness must be created to form their experience before they enter the workforce [7]. Academic institutions are an important part of preparing and educating the cybersecurity workforce. The current research aims to enhance the awareness of University students about the correct practices in cybersecurity, the students were selected because they are the future employees of the organizations [8].

This paper is organized into six sections. Section 2 explains the awareness concept, Section 3 Explains the most famous cyber threats and their types, Section 4 discusses previous studies that focused on cyber threats caused by the human factor, and Cyber Security Enhancement Factors, The importance of cybersecurity awareness in universities. Section 5 Discussion of relevant studies and finally Section 6 Conclusion and future directions.

2. AWARENESS

The concept of awareness first appeared in the theory of innovation diffusion [9], and awareness is defined as the extent to which the target population is aware and the formulation of a general perception of what it entails, and this means that awareness is a precedent for behavioral attitudes and intentions [10]. Situation Awareness SA, defined according to [11], is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status shortly. As explained by [12] situational awareness is on three hierarchical levels of situation assessment, each stage being a precursor to the next higher level. He mentioned [4] levels of situational awareness in (figure 1) as follows:

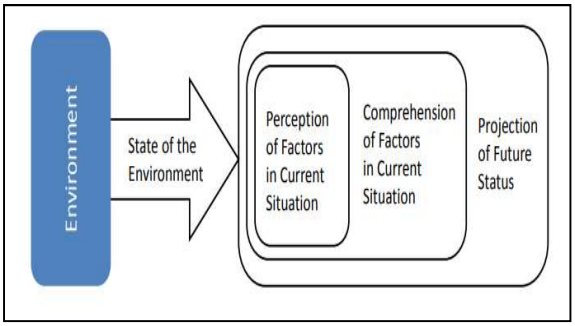

Figure 1: Layers of situational awareness.

2.1 Perception

The first layer includes perceptions of the critical factors in the environment that are important to the decision-maker. Perception involves assessing and defining the state, characteristics, and dynamics of relevant factors in time and space based on data collected from various sources in the environment.

2.2 Comprehension

The second layer includes the factors of the first layer. It includes the integration, understanding, and association of the disjointed elements that must be understood to make a sound decision in the context of the decision maker's role.

2.3 Projection

The third layer presents understanding the situation in the future to predict the impact of those elements in the future decision context of the decision maker's vision. Both the first and second layers of management and projection involve knowledge of the state and dynamics of factors and an understanding of the elements that characterize a situation to predict what will happen in the environment over some time.

[13] described it as a model that presents situational awareness as a dynamic interaction between the environment and humans. Also, the information processing approach is best represented by it, the three-level model of situational awareness was developed to understand flight tasks [14]. With technological development, it can be used to regulate human performance, and in behavior that requires cognitive tasks, to increase the capabilities of humans to act as decision-makers [12].

3. CYBERSECURITY

The International Telecommunication Union (ITU) defines cyber security as a set of security concepts, policies, tools, guidelines, security guarantees, and best practices that can be used to protect the organization's assets, the user, and the cyber environment [15]. The authors in [1] defined cybersecurity as the process that includes several different processes in protecting basic software, processes, and technologies, data from damage, infection, or unauthorized access, people, and devices. considering the different types of components of cyberspace, cybersecurity should cover the following attributes: safety, confidentiality, availability, reliability, integrity, maintainability (of physical networks, systems, and information) survivability and resilience (to support the dynamism of cyberspace), credibility, non-repudiation, and accountability, (to support information security) [16]. Also, Cybersecurity is considered to be one of the main challenges for anyone connected to the Internet, however, public awareness of cybersecurity is still limited [17].

3.1 Challenges to cybersecurity

In recent years, cyber threats and social attacks have increased dramatically, making organizations increase their efforts to mitigate or prevent these threats. The quality of interrelated influences that occur between components of the human factors system may affect overall human performance and actions. Poor management practices, poorly written rules, and unclear procedures can have many negative effects. Cybersecurity challenges can be described from a socio-technical perspective, taking into account the multiple perspectives of organizational factors, individual factors, technological factors, and ethical dimensions to the following:

3.1.1 the organizational factor

In any organization, there are formal policies, processes, and procedures to guide employees in keeping the system secure. When corporate employees fail to follow them, the organization is held accountable. However, formal procedures do not rule over human behavior [18]. However, humans can configure and employ a system in unprotected modes, or unexpected and take shortcuts for the sake of efficiency or for the sake of just being helpful even if it involves enforcing a violation. If employees are unsure of how to implement policies and rules in the real world or are deemed too costly to follow, they rely on informal procedures and intuitive costs and thus do not adhere to recommended policies [19]. The information security culture of an organization influences how management handles and treats security problems. A strong information security culture offers a means of minimizing the risk from employee behavior while interacting with and processing information[20]. Also, the organizational culture and the top management's interest and attention to these aspects can influence HF-related risks of cyber threats and attacks[19].

3.1.2 the individual factor

Providing incorrect security involves the risk of errors and violations. While a limited number of them are malicious (e.g., sabotage), most are the result of unintentional problems caused by an inappropriate arrangement of work elements. To analyze systematic individual variance associated with the probability of occurrence of error-causing conditions and violations, several psychological frameworks can be used. According to models of rational action theory and planned behavior theory linking behaviors and attitudes through a mediating effect called behavioral intent, it is possible to explain human errors and violations by studying employee attitudes toward behaviors critical to cybersecurity, since cybersecurity can be improved, as attitudes directly predict intention Actual behavior of unsafe behaviors [19]. Table1 illustrates the classification of human errors and violations.

Table 1: Taxonomy of Human Errors and Violations.

Incorrect security actions	Error/violation type	Description
Accidental and non-deliberate actions determining a violation of a security rule	Slips skill-based	Incorrect actions in tasks that are routine and require only occasional conscious checks; these errors are related to the attention of the individual performing actions relevant for security.
	Lapses skill-based	Memory failures in actions relevant for security, such as omitting a planned action, losing one's place, or forgetting security-relevant intentions.

Deliberate actions determining an unwanted violation of a security rule.	Rule-based mistakes	Application of a bad rule relevant for security Inappropriate application of a good rule relevant for security.
	Knowledge-based mistakes	An intentional act involving faulty conceptual knowledge, incomplete knowledge, or incorrect action specification, leading to the unwanted violation of a security policy or procedure.
Deliberate violations of a security procedure with no malicious intent.	Violations	Intentional deviation from security policies or procedures due to underestimation of security consequences (can be either routine or exceptional).
Deliberate violations of a security procedure with malicious intent.	Malicious	violations Intentional deviation from security policies or procedures to sabotage the system.

3.1.3 the technological factor

Implementation of user experience principles to improve usability remains an open issue with the current implementation of CIS in organizations while security is user-focused, users still actively avoid hard-to-use security mechanisms and make mistakes that undermine security. About keeping data, systems, and devices safe for vulnerable groups, it was said that cybersecurity can be a barrier to usability. [19]. with the increasing number of electronic health care information databases, it has had its drawbacks and advantages, as it has helped improve communication between healthcare institutions and practitioners[22]. However, several concerns emerged regarding the relationship between professionals, patients, and health care providers, the available capacity and protection of it, and how confidentiality and integrity are managed.

3.2 Cyber Threats and Attacks

The tremendous growth in modern technologies, especially communication applications used to disseminate information and communicate with others on a large scale, has led to an increase in cyber threats and electronic attacks, in addition to the diversity of methods and methods of hacking, which are renewed periodically. However, customer demands have increased for the private and public sectors to provide technologies and services to provide access to information anywhere and at any time. The types of cyber threats can be either human or non-human events as shown in (figure 2). Non-human events include natural disasters like fires, earthquakes, electrical power loss, hard disk failures, etc. While human threats are benign or malicious, benign threats are the result of accidents and indirect human errors like mistyping a command, while malicious acts result from Bad intentions[21].

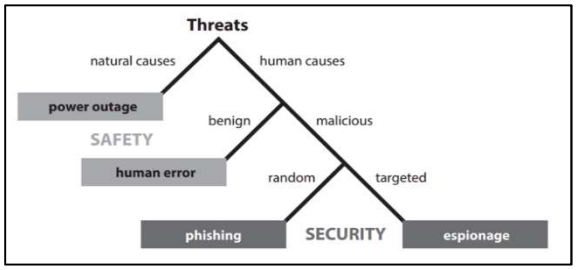

Figure 2: Types of Threats.

The percentage of organized cybercrime groups and the number of hackers has increased dramatically, and cybercriminals are relying on new methods to carry out cybercrime. Where financial gains were the main motive for hacking, and one of the ways hackers use to get money is to steal sensitive information and keep it to demand a ransom from the victim. Also, one of the ways they use to make money is to sell confidential data to competitors on the dark web, and this makes cyberspace unsafe and leads to great risks to customers and institutions. Also, cybersecurity violations posed a serious threat to economic and global security, due to their targeting of vital infrastructure that has a significant impact on business performance, which leads to a significant loss of intellectual property [23]. Phishing is a method of social engineering that appears among the top 5 cyber threats of 2020 [24].

3.3 Social Engineering

The author said in [25] that Social engineering is the most common type of cyber threat over the Internet to target victims which include:

1. Phishing: Scams attempt to obtain personal information such as addresses and other personally identifiable information (PII) such as Social Security numbers and names. Phishing scams include links to redirect users to suspicious websites

that appear legitimate. These types of tricks create a sense of urgency to manipulate users into behaving in a way that defies good judgment.

2. Pretexting: It is a type of social engineering attack driven by a fabrication scenario that attempts to confirm and steal personal information from a target leaving no room for suspicion of the target, as advanced attacks try to exploit a weakness in an organization or company. The strategy is to use urgency and fear while building a sense of trust with the victim to ensure that the required information is obtained.

3. Baiting: Similar to a phishing attack, it offers lure strategies to a victim. Hackers use the lure of promised goods if the user hands over login credentials to a particular site.

4. Quid pro quo: This type of threat is presented as a technical service in exchange for information, in which the attacker impersonates an IT representative and provides assistance to the victim who may face technical challenges, then the attacker releases malware on the user's system.

5. Tailgating: This type of attack uses oscillation and backscattering to reach restricted areas. This attack exposes those with access to a restricted area to an attacker who may impersonate delivery personnel who need temporary access. Data breaches are one of the most harmful cyberattacks, As shown in (figure 3).

Figure 3: Losses caused by cyber threats.

The authors in [18] claimed that there are three main cyber targets, called the Confidentiality Integrity Availability triad (CIA) :

1. Confidentiality threat (data theft) that can target application servers, databases, backups, and system administrators.
2. Integrity threat (altering of data) includes hijacking, theft of large sums of money, alteration of financial data, direct deposit redirection, and damage to the image of the organization.
3. Availability (Access Denial) attacks can be distributed denial of service (DDoS), targeted denial of service, and physical destruction.

3.4 Cyber-Attacks in the Kingdom of Saudi Arabia

One of the fastest developing countries in the Middle East is Saudi Arabia, which uses technology as an important resource in every aspect of development. Internet technologies are used in public sectors and other institutions such as schools, hospitals, and other private institutions ‹Internet penetration increased to 65.9% and more and more than 18 million users of the Internet and 12 million users of Facebook, and the number is increasing. Social networking is one of the highly engaged aspects of internet use, with Facebook and Twitter being popular in the region. Also, about 39% (12% of the total population) of adult internet users buy products online and pay online for services ‹making their bank statements vulnerable to hacking and cyber risk [16].

The Kingdom of Saudi Arabia is the second largest e-commerce market in the Middle East, with a statistic of $520 million, With the increase in advanced sophistication and innovative cyber-attacks launched by hacker activists and foreign governments, business organizations and government agencies have faced huge challenges in the country, in 2012, a cyber attack occurred that targeted the oil and gas company and one of the main sources of income for the Saudi government, which is called Saudi Aramco, which damaged nearly 30,000 computers, using the Shamoon malware, which is considered one of the most destructive cyberattacks targeting a single company. Also ‹a series of attacks emerged in 2013 targeting various government websites including the Ministry of Interior website. In 2015, Saudi Arabia experienced 60 million cyber-attacks, it was expected that cyber-attacks would increase rapidly, as hackers change their tactics and strategy daily. In 2017, Saudi Arabia's General Entertainment Authority (GEA) also fell victim to cyber-attacks. The National Cyber Security Center (NCSC) explained that there is a new advanced cyber-attack using PowerShell malware through phishing email targeting Saudi government agencies causing a lot of disruption to services[16].

4. LITERATURE REVIEW

4.1 Cyber Threats caused by the Human Factor

The author said in [26] discussed highlighted pitfalls and ongoing issues that organizations encounter in the process of developing human knowledge to protect from social engineering attacks. That despite state-of-the-art

cybersecurity preparations and trained personnel, hackers are still successful in their malicious acts of stealing sensitive information that is crucial to organizations. The factors influencing users' proficiency in threat detection and mitigation have been identified as a business environmental, social, political, constitutional, organizational, economic, and personal.

The study found the need to classify employees at risk after analyzing the challenges related to both traditional and modern tools and developing training programs to ensure that the hackers' actions do not succeed. In addition, it is practically impossible to eradicate social engineering violations without working to improve the level of information security awareness among all employees to address human cybersecurity risks.

Researchers claimed in [27] that there are many modern communication applications, but the person's e-mail is still the online identity. The study aimed to show the security shortcomings in an e-mail. Which enables malicious actors to commit fraud through phishing emails. Technical solutions do not completely solve this problem, so users need to be trained on how to identify and respond to suspected fraudulent emails. The study described the essential components of a comprehensive program that tests, trains, measures, and enhances an organization's cybersecurity to defend against and mitigate phishing attacks. The program relied on the author's operational experience in publishing and implementing training programs and working with best practices recommended by the National Institute of Standards and Technology. The most important finding of the study is the importance of implementing a comprehensive phishing training program along with email security technology. To improve the overall cybersecurity situation and reduce the possibility of a cybersecurity attack caused by fraudulent emails.

4.2 Cyber Security Enhancement Factors

The author mentions in [28] aimed to describe the factors that can be good in promoting cyber security awareness campaigns: First, security awareness must be professionally prepared and organized to operate. Second, invoking fear in people is not an effective off-the-shelf technique, as it may frighten people less able to take risks. Third, security education should be more than just providing information to users - it should be targeted, actionable, actionable, and provide feedback. Fourth, once people are ready for change, training and constant feedback are essential to keep them going through the change period. Fifth, the focus is necessary on different cultural contexts and characteristics when creating cybersecurity awareness campaigns. The findings of the study the importance of thinking critically about the challenges involved in improving the information security behaviors of employees, citizens, and consumers. Understanding how people perceive cyber risks is critical to creating effective awareness campaigns.

Researchers claimed in [29] discussed the concept of cyber defense exercises (CDX). Which contribute to promoting awareness of the safety of cyberspace, collecting empirical experiences, and testing the organization's ability to resist and respond to cyber events to create a secure environment. The cyber defense exercise includes four categories: First, to test and improve national and international cooperation in responding to cyber incidents. Second, assess competition in cybersecurity skills, and the preparedness of individuals, organizations, and systems for incidents. Third, is the assessment of technical ability. Fourthly. Training participants in real-world scenarios provide the opportunity to gain knowledge and experience by developing their skills and resilience before an incident occurs. The exercises give ideas to decision-makers from officials, institutions, organizations, and responsible employees about precautions in the field of cybersecurity and the cyber techniques, tools, and procedures that can be developed.

The results concluded that all that there was continuous training on cyber defense helps in activating awareness of cyber defense and detecting weaknesses in the field of cyberspace, in addition to the integrated techniques that can be followed in the exercises related to cyber. The author mentions in [30] aimed to find out the importance of educating contemporary learners on the dangers of cyberspace and the strategies that can be used how to promote and teach cybersecurity in schools. The advent of the Internet has positively affected people's lives, but it was the cause of negative problems related to the use of the Internet. Such as to internet addiction, teens spend a lot of time on social media and computers. Adults were surveyed to determine their willingness to learn and educate about cybersecurity.

The results of the study indicate the importance of cybersecurity education in schools, as a survey of adults indicated that participants are not willing to spend time and money on seminars or programs on cybersecurity. Video animation is one

of the most prominent strategies that can be used to enhance cybersecurity education in schools, as teachers use it when discussing cybersecurity to raise cybersecurity awareness. Also, holding weeks to raise awareness of cyber security and to teach safety aspects of cyber security. In addition to the importance of the cooperation of all relevant parties including parents, government, and teachers, to find the best solution to protect children from cybercrime through cyber security education in the school. In the future, the study made it clear that the future source of the state for electronic defense is for people trained in cybersecurity.

The author said in [31]aimed to present the strategies that frame cyber security in a way that generates more societal and political awareness. The strategies were based on each of the more general literature such as linking cybersecurity with values other than security. Investing in cybersecurity can yield economic benefits because countries that invest in fighting cybercrime will build valuable expertise. Also, personalization for Ease of Recognition Where message customization is an important framing strategy, which should ensure that the problem is recognized in everyday life.
The results were, that cybersecurity needs to be framed not only as a problem-solving task but for creating economic opportunities, which could make it attractive to invest in expertise in cybercrime. Whenever complex and abstract topics such as cyber security are relevant to people's immediate living environment, they will easily realize the need to tackle cyber security. For example, companies in the high-tech industry are more receptive to the threats of espionage and the risk of their ideas being stolen and used by other organizations, while citizens will better understand the need when faced with the possibility of credit card theft or blocking and the risk of losing money. So, both groups also require different tools to ensure their safety in cyberspace.

The author mentions in [32] explained the proposed approach Analyze Predict Aware Test (APAT) approach to protecting the important assets of the organization as follows: Firstly, Analyze the Trend: They analyzed according to cybersecurity guidelines from NCIIPC, that the top three vulnerabilities are phishing, malware, and suspicious software, and 90% of cyber-attacks are caused by human negligence. Secondly, Predict the Behavior: After the analysis process, they note that human negligence is the cause of cyber-attacks / bug that leads to attacks like social engineering, phishing, etc. Third, Awareness based on User profile: Awareness of information security through 1–2-hour training can only provide some basic aspects of information security so it cannot be made to increase employee culture. Finally, Test the Effectiveness: The basic step in building a security awareness program is the cyber security awareness test to form a baseline by conducting some assessment tests to check employee awareness and start building the awareness program. To verify the effectiveness of the program, used the success tracking equation that tracks how effectively the solution has been implemented to attract awareness of cybersecurity.

The results of an APAT model are developing a culture focused on security, reducing the falling victim to phishing and fraud campaigns, and can help an organization improve existing cybersecurity practices or develop new processes.
The author said in [33] aimed to conduct an opinion poll to measure students' awareness of cybersecurity. In the research methodology, the study relied on a questionnaire, to find out the extent of awareness among students among three age groups from 8 years to 21 years. The questionnaire included several questions about the concepts of cybersecurity and the use of the Internet, on both smartphones, tablets, desktops, and laptops.

Survey results indicate that awareness of cybersecurity among the students surveyed was generally low among the three categories. Most of the students did not have sufficient knowledge of cyber security terminology as well as they did not have sufficient awareness of common threats such as phishing, or knowledge of cyber security tools for smartphones and tablets. Stressed the need to create awareness of cyber security for students in the school to overcome cyber threats.

4.3 The Importance of Cybersecurity Awareness in Universities

Researchers claimed in [7] whose aim is to measure the level of awareness of Saudi university students about cybersecurity, a questionnaire was designed in which 136 students participated and it measures students' awareness through their culture, the surrounding environment, and their knowledge, in addition to the students' behavior.
The results indicated a medium level of awareness of cyber security among students and that cyber security receives more attention among female students. In addition, the students in computers and information technology had a higher awareness compared to the students in other departments. The authors emphasized the importance of providing

cybersecurity awareness to university students and that they should be aware of potential threats while using the Internet.

Students are exposed to data breaches due to the lack of awareness of cybercrime. Therefore, the study [23] aimed to assess the level of cybersecurity awareness and user compliance among undergraduate students at Majmaah University. Through an online questionnaire, which depended in its design on the safety factors of using the Internet, 576 students participated in it. The results of the study indicated that a cybersecurity awareness program should be included for students and that academic institutions need several training courses and security awareness sessions to ensure that all students are aware of cyber threats.

The author said in [34]aimed to provide a comprehensive study into how risk preferences, decision-making patterns, and behaviors related to safety and insurance influence. The research methodology was based on a questionnaire where the survey included 369 faculty members, students, and employees of a large public university. They linked cybersecurity behavior intentions to four main categories of individual differences: risk preferences, decision-making styles, personality traits, and demographics. They found that individual differences accounted for 5%-23% of the variance in intent or cybersecurity behavior.

The results were that universities fall victim to cyber-attacks, and that rational decision-making and gender are important factors for predicting the intentions of good security behavior. Also, previously unreported outcomes such as financial risk were found to be an important indicator of good password generation behavior.

Researchers claimed in [35] aimed to find out how students perceive cyber-attacks and how they can mitigate the attacks and to know if the cybersecurity awareness program is part of the university program. The study objectives included determining the level of basic knowledge of cybersecurity among university students in Nigeria, determining whether cybersecurity is among their curricula, and also determining whether a cybersecurity awareness program is required. The quantitative approach was used in the study in designing a questionnaire to collect data, and the student participants were chosen because they are future employees in any institution.

The study result indicated that there is no approach in place to increase the level of cybersecurity awareness for students in universities in Nigeria and that students lack basic knowledge of cybersecurity and phishing attacks. The study also focused on the urgent need to conduct a cybersecurity awareness program and also include it as a core course at the university level in Nigeria and those students demand such awareness of cybersecurity. Also, similar research was conducted in different countries, including Malaysia and the United States, to find out the level of cybersecurity. All results indicated a lack of awareness of cybersecurity and the need for an awareness program to increase the level of awareness and reduce successful cyber-attacks in universities.

5. DISCUSSION

In recent years, cyber threats have increased dramatically. Among the top 5, the most common threats of 2020 were social engineering. Social engineering refers to the design and application of deceptive techniques for the intentional manipulation of human targets. In the context of cybersecurity, it is used primarily to urge to disclose confidential data, implement victims measures that violate security protocols, infecting systems without knowing or releasing classified information[24]. The study [26]discussed the issues that organizations face in the process of developing human knowledge to protect against social engineering attacks. While the study [36] shows that the threats of social engineering are among the most serious security violations that organizations are exposed to. In the study [27], he focused on showing the security shortcomings in the e-mail that enable malicious actors to commit fraud through phishing e-mails to humans. The studies [26] [36] agreed with the current study on the need to work on improving the level of awareness to face human cybersecurity risks. Using methods to mitigate threats that include the use of cybersecurity training and awareness methods.

While the study [27] had a similar orientation to the current study in that technical solutions cannot solve the fraud and deception methods that humans are exposed to, by enhancing their level of awareness and training to face these threats, these threats can be reduced and possibly eliminated in the future.

In the study [28], the important factors in strengthening cybersecurity awareness campaigns were clarified. In a study[29] I explained the concept of cyber defense exercises (CDX) that help in enhancing awareness of cyberspace safety and testing the organization's ability to resist and

respond to cyber events to create a secure environment. The study [28] [29] constitutes the starting point for implementing effective awareness programs, and it is the future goal of the current study.

In the study [32], in which they presented a model (APAT) to measure awareness of cyber security, this model is useful for measuring the level of awareness as applied by the study [7]. The study [32]has the same direction as the current study in that 90% of cyber-attacks are caused by human negligence. Therefore, whenever there is a focus on enhancing awareness of cybersecurity in addition to developing technical solutions to confront threats, it helps to reach safe cyberspace. In a study [30][33] researchers focused on the importance of enhancing and teaching cybersecurity in schools. Therefore, the current study focused on the importance of early awareness among students, because of its positive impact on themselves and their environment. In a study [31] he explains a way to generate more societal and political awareness by presenting strategies that frame cybersecurity. The Studies [28,29,31 and 32] reinforce the directions of the current study in highlighting the enhancement of cybersecurity.

The Studies [7,21,32, and 33] Similar to the current study focus on the lack of awareness of cybersecurity and the emphasis the need for an awareness program to raise the level of awareness and reduce cyber-attacks in universities. In addition, a cyber security awareness program must be included for students, and academic institutions need many training courses and security awareness sessions to ensure that all students are aware of cyber threats.

Therefore, raising students' awareness of cybersecurity, its threats, and risks, enhances students' references to action when confronting cybercrime to protect information and technology assets. It also motivates students to participate in security training that helps students build their expertise in the field of information security. In addition to preparing them to enter the labor market with sufficient cybersecurity awareness.

6. VALUE OF THIS STUDY

The literature review revealed that there is a lack of research that discusses cybersecurity awareness among higher education students and the importance of cybersecurity awareness. Previous studies discussed the importance of providing cybersecurity awareness among employees, and the importance of cyber security education in schools. Also, cyber threats are caused by a lack of awareness of the human factor and cyber threats that have appeared very widely such as social engineering as scams through phishing emails. The current study dealt with the problem of limited awareness of cyber security among university students in Saudi Arabia. However, today students are future employees, so they must be aware enough of cyber threats and how to deal with them to reach safe cyberspace.

It then based on the few studies that discussed the awareness of cyber security among university students and the importance of providing awareness raising among university students. The result of this study indicates the need to provide awareness of cyber security among university students, such as creating a website that contains the correct policies and practices for topics that students are vulnerable to plagiarism through.

7. FUTURE RESEARCH DIRECTIONS F

One of the future directions is a study of the reality of privacy practice and its relationship to cybercrime among different age groups among university students. The second direction is comparing the level of awareness of the students of computers college in cybersecurity with the students of other colleges. The third direction is knowing the factors that enhance cybersecurity awareness among universities students in the Saudi Arabia and provide a platform for cyber security awareness and correct practices to confront cyber threats in each university, with the addition of incentives for students such as a certificate of attendance that increases the student's CV, also to make sure that the student has acquired sufficient awareness of cybersecurity, through his assessment or a test.

8. CONCLUSION

The rate of cyber threats and cybercrime is increasing due to the digital transformations that the world is witnessing. Because university students make up the majority of those who use the network in Saudi Arabia, this research emphasized the significance of raising cyber security knowledge among them. However, the current study did not identify the factors to enhance cybersecurity awareness among university students, it did not measure the level of awareness of Saudi universities students about cybersecurity. The findings of this study show that cyber security knowledge is vital for ensuring the protection and privacy of sensitive information assets. However, technical solutions cannot solve the fraud problem that people are exposed to. Enhancing cyber security awareness should be provided to universities students to create

an experience for them to face cyber threats to reach safe cyberspace to achieve the Saudi Arabia Vision of 2030.

REFERENCES:

[1] R. E. Beyer and B. J. Brummel, "Implementing effective cyber security training for end users of computer networks," *SHRM-SIOP Sci. HR Ser. Promot. Evidence-Based HR*, 2015, [Online]. Available: https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP Role of Human Resources in Cyber Security.pdf.

[2] E. C. Controls, "Essential-Cybersecurity-Controls," vol. 2018, 2018.

[3] Euler Hermes, "Saudi Arabia Country Risk Report & Analysis," 2017, [Online]. Available: https://www.eulerhermes.com/en_CA/resources/country-reports/Saudi-Arabia.html#link_internal_1.

[4] H. Tianfield, "Cyber Security Situational Awareness," *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pp. 782–787, 2017.

[5] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, 2020.

[6] V. D. Andrews, "CSU ePress In-Depth Analysis of College Students ' Data Privacy Awareness," 2020.

[7] W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, "Cybersecurity Awareness Level: The Case of Saudi Arabia University Students," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 3, pp. 276–281, 2021.

[8] A. Garba, M. A. Musa, and S. H. Othman, "A Study on Cybersecurity Awareness Among Students in Yobe : A Quantitative," no. July, 2020.

[9] E. M. Rogers, "17 - Rogers 1995 cap 6.pdf." p. 26, 1995.

[10] T. Dinev and Q. Hu, "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *J. Assoc. Inf. Syst.*, vol. 8, no. 7, pp. 386–408, 2007.

[11] C. Macabante, S. Wei, and D. Schuster, "Elements of Cyber-Cognitive Situation Awareness in Organizations," pp. 1624–1628, 2019.

[12] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Hum. Error Aviat.*, vol. 37, no. March 1995, pp. 217–249, 2017.

[13] "Copyright ©2000. All Rights Reserved.," 2000.

[14] N. A. Stanton, P. R. G. Chambers, and J. Piggott, "Situational awareness and safety," *Saf. Sci.*, vol. 39, no. 3, pp. 189–204, 2001.

[15] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *Int. J. Child-Computer Interact.*, vol. 30, p. 100343, 2021.

[16] F. Fahad, "Evaluation and Enhancement of Public Cyber Security Awareness," 2019.

[17] H. de Bruijn and M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," *Gov. Inf. Q.*, vol. 34, no. 1, pp. 1–7, 2017.

[18] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, 2020.

[19] A. Pollini *et al.*, "Leveraging human factors in cybersecurity: an integrated methodological approach," no. 0123456789, 2021.

[20] S. Review and N. Martins, "Accepted Manuscript (Unedited)," pp. 243–256, 2015.

[21] B. Gordijn, M. Christen, and M. Loi, *The Ethics of Cybersecurity*, vol. 49, no. 0. 2020.

[22] I. M. Management and E. Url, "Northumbria Research Link," pp. 25–35, 2018.

[23] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of Majmaah University," *Big Data Cogn. Comput.*, vol. 5, no. 2, 2021.

[24] F. Breda, H. Barbosa, and T. Morais, "SOCIAL ENGINEERING AND CYBER SECURITY," 2016.

[25] N. Y. Conteh and P. J. Schmick, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, pp. 31–38, 2016.

[26] H. Aldawood and G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs — Pitfalls and Ongoing Issues," 2019.

[27] M. J. A. Miranda, "Enhancing Cybersecurity Awareness Training : A Comprehensive Phishing Exercise Approach," vol. 14, no. 2, pp. 5–10, 2018.

[28] M. Bada, A. M. Sasse, and J. R. C. Nurse,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

"Cyber Security Awareness Campaigns : Why do they fail to change behaviour ?"
[29] E. Seker, "The Concept of Cyber Defence Exercises (CDX): Planning , Execution , Evaluation," no. Cdx.
[30] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The Importance of Cybersecurity Education in School," vol. 10, no. 5, 2020.
[31] H. De Bruijn and M. Janssen, "Building cybersecurity awareness : The need for evidence-based framing strategies," *Gov. Inf. Q.*, vol. 34, no. 1, pp. 1–7, 2017.
[32] A. H. Khan, P. B. Sawhney, S. Das, and D. Pandey, "SartCyber Security Awareness Measurement Model (APAT)," *2020 Int. Conf. Power Electron. IoT Appl. Renew. Energy its Control. PARC 2020*, pp. 298–302, 2020.
[33] A. Sarrafzadeh and P. Pang, "A survey on Internet usage and cybersecurity awareness in students."
[34] U. States, B. Sketches, and I. Technology, "Correlating Human Traits and Cybersecurity Behavior Intentions," pp. 1–20, 2017.
[35] A. Garba, Maheyzah Binti Sirat, Siti Hajar, and Ibrahim Bukar Dauda, "Cyber Security Awareness Among University Students: A Case Study," *Sci. Proc. Ser.*, vol. 2, no. 1, pp. 82–86, 2020.
[36] H. Aldawood and G. Skinner, "An Academic Review of Current Industrial and Commercial Cyber Security Social An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions," no. October, 2019.