The Effectiveness of Counselling Program develop awareness of cybersecurity among Internet users among secondary school students in Riyadh Region's

By

Prof Saad Abdullah S Al- Moshawah * Prof Abd El. Mureed Abd ElGabr Qasem**

Samoshawah@imamu.edu.sa aaamkasm@imamu.edu.sa

ORCID:0009-0000-9637-3976

* Department of Psychology - Faculty of Social Sciences * Imam Mohammad Ibn Saud Islamic (IMSIU) , Riyadh. Saudi Arabia

** Department of Psychology - Faculty of Social Sciences - Imam Mohammad Ibn Saud Islamic (IMSIU) , Riyadh. Saudi Arabia

Abstract : This research aims to evaluate the efficacy of a counselling program in fostering cybersecurity awareness among secondary school students in Riyadh Region's, Saudi Arabia. The program's impact on internet users within this specific population will be the primary focus. The sample comprised 30 secondary school students from Riyadh schools, evenly divided into an experimental group (n=15) and a control group (n=15). A cybersecurity awareness test developed by Noura Al-Sanea et al. (2020) was employed. An indicative program designed to cultivate cybersecurity awareness was implemented. The results revealed statistically significant differences ($p<0.001$) between pre- and post-test scores on the cybersecurity awareness test within the experimental group following the program's application. These differences favored the post-test scores, indicating the program's effectiveness. While the study identified statistically significant differences ($p < 0.001$) on the post-cybersecurity awareness test scores between the experimental and control groups, further analysis is needed to determine the direction of these differences.

Keywords: *awareness* of *cyber security*. Counselling Program.

Introduction:

Over the past decade, information technology has revolutionized the utilization of digital applications on communication devices, significantly simplifying various aspects of daily life. This transformation is evident in areas such as digital newspaper readership, the educational process, tourism, consumer behavior, and in offering support and recommendations to decision makers (Sabillon et al., 2021).

With the rapid advancement and widespread adoption of modern information technologies across various facets of life in all societies, cybersecurity threats have emerged as significant challenges, greatly impacting information security. Identifying the types of these threats has become increasingly difficult (Alzubaidi, 2021).

In their simplest form, these threats are unintentionally executed by individuals with technological skills. However, the severity escalates when carried out by malicious groups of hackers and terrorists who possess the expertise to attack information systems. These threats frequently result in social and economic losses for the affected communities. As the number of internet users continues to rise, the gravity of cyber threats also increases, making the pursuit of cybersecurity critically important (Bordoff et al., 2017).

Despite the expertise of many technology companies in combating cybersecurity threats, accurately cataloging these threats has become nearly impossible. The dynamic and ever-evolving nature of these threats ensures that new forms continuously emerge..

The persistence of cybersecurity threats, even in the face of advanced technological countermeasures, has underscored a critical vulnerability: the human factor. From a psychological perspective, security specialists now recognize that human behavior represents the weakest link in the cybersecurity chain. Psychology plays a vital role in mitigating cyber threats. Effective cybersecurity goes beyond just technology; it requires a focus on understanding human behavior and psychology. After all, even the most sophisticated security systems cannot eliminate the risk of human error and social engineering tactics.

This human factor also plays a significant role in cybercrime (Wiederhold et al., 2014). Psychologists can leverage their expertise to bolster cybersecurity by understanding the diverse psychological profiles of internet users. This includes analyzing their risk assessment capabilities. Research by Hadlington & Parsons (2017) underscores this point: only 23% of users effectively navigate real-world cybersecurity scenarios, and a mere 4% can handle over 90% of such situations.

Furthermore, the burgeoning accessibility of the internet coincides with a rise in adolescent internet usage. This increased exposure unfortunately translates into a heightened vulnerability to cyber threats for this age group.
.

The rise of Generation Z (born between 2001 and 2013) merits mention in the context of cybersecurity awareness. Often characterized as digital natives due to their immersion in the internet from a young age, this generation exhibits a high degree of technological fluency. However, research suggests a potential paradox: despite their familiarity with technology, Gen Z may be susceptible to certain online threats. Factors contributing to this vulnerability could include their dependence on social media platforms and a possible lack of awareness regarding cybersecurity best practices.

The aforementioned considerations highlight the critical need to cultivate cybersecurity awareness and mitigate cyber threats to information security among internet users, particularly teenagers.

Training and guidance programs offer a promising solution. While the field of cyber psychology remains nascent, training programs designed to cultivate cybersecurity awareness have emerged. These programs are rooted in research that identifies key psychological factors influencing success or failure in achieving cybersecurity (Bordoff et al., 2017).

This recognition of the human element in cybersecurity vulnerabilities has driven researchers to explore the potential of psychological counselling techniques. These techniques aim to mitigate the severity of cyber threats by fostering a heightened awareness of the diverse cyber risks faced by internet users, particularly teenagers..

The contemporary world is experiencing a confluence of factors: rapid advancements in communication technologies, ubiquitous internet access, and a flourishing digital information exchange. Unfortunately, this interconnectedness coincides with a rise in cyberwarfare, mirroring traditional warfare but with digital weapons. Cyberattacks have become as commonplace as internet usage itself. In fact, their frequency is demonstrably increasing, as evidenced by news reports and academic research highlighting a surge in the volume and diversity of attacks and cybercrimes. A significant contributing factor to this alarming trend is the lack of user understanding and awareness regarding internet risks and appropriate mitigation strategies (Raineri & Resig, 2020).

It's important to acknowledge the specific context of this study: the Kingdom of Saudi Arabia. The nation has unfortunately witnessed significant infrastructure damage due to cyberattacks. The most prominent example is the series of attacks targeting Saudi Aramco, which disrupted its operations for a month. This incident, considered the largest hack in history, involved malware that caused further malfunctions within the company in November 2016 and January 2017 (Ibrahim, 2021).

The Kingdom of Saudi Arabia has embraced a comprehensive cybersecurity strategy aligned with Vision 2030 and national strategic goals. This approach prioritizes the protection of its cyberspace and critical infrastructure, fostering a secure environment for achieving Vision 2030's objectives.

Furthermore, the strategy emphasizes the development and implementation of cybersecurity principles across all government agencies, private sectors, and society as a whole. By fostering awareness and promoting responsible practices among individuals and entities, this collaborative approach strengthens the nation's cyber resilience (National Cybersecurity Authority, 2021).

On a global scale, significant efforts are underway to combat internet risks and safeguard sensitive information. These efforts prioritize the confidentiality, integrity, and availability of data in the face of the ever-present challenges of the digital age. Organizations worldwide have invested heavily in technological countermeasures for information security.

However, the success rate has been mixed. This lack of complete protection, despite significant investment, suggests an over-reliance on solely technical solutions, which may be insufficient to address the evolving landscape of cyber threats (Raineri & Resig, 2020).

For a more nuanced understanding, it's crucial to acknowledge that a significant portion of information security incidents stem from the manipulation of human vulnerabilities. These human factors, whether directly or indirectly, contribute to the majority of cyberattacks. Consequently, fostering individual information security awareness (ISA) emerges as a critical element in safeguarding against malicious activities (Khando et al., 2021).

It's worth emphasizing that the human element remains the most vexing challenge for cybersecurity researchers and practitioners worldwide. The vast majority of cyber incidents can be attributed to user behavior, with attackers actively exploiting these vulnerabilities. This stark reality underscores the limitations of current technological information security measures (Raineri & Resig, 2020).

Psychological research on cyberattacks highlights a critical factor in their success: the lack of awareness among many internet users regarding diverse online threats, often referred to as "electronic risks." This deficiency in awareness often translates into a reluctance to adopt cybersecurity safeguards, ultimately compromising information security and confidentiality on their devices (Bada & Nurse, 2020; Halevi et al., 2016; Odemis et al., 2022; Seigfried-Spellar et al., 2015).

Given this reality, cultivating cybersecurity awareness has become an imperative. This is demonstrably evident in the growing emphasis organizations place on enhancing such awareness. By fostering this awareness, individual and organizational attitudes shift, leading to a deeper understanding of the importance of security and the potential consequences of cyber threats.

In the realm of information and communication technology security, awareness is paramount. A user's actions can have far-reaching consequences for the entire organization. As Yunus et al. (2016) point out, an unaware user, particularly one in a position of authority, can inflict serious damage.

It is noteworthy that the researcher's attention was drawn to a scientific report indicating that teenagers of both sexes constitute the largest age group using the Internet in the context of the current study. According to the results of a Saudi study conducted by Al-Ruwais (2013), the percentage of internet use among Saudi teenagers is significant. These young users often utilize the internet ahead of schedule, driven by advancements in communication technology and social networking platforms. Consequently, the field of smartphones and computers has witnessed a high level of technological development.

Recent data indicate that American high school adolescents are most frequently cyber-victimized on social networking sites (62%) and through text messages or other messaging platforms (40%) (Waasdorp & Bradshaw, 2015). From this perspective, it has become essential to develop programs aimed at increasing cybersecurity awareness.

Given the complexity of cyber threats and their psychological and social consequences, it is crucial to consider the challenges hindering the improvement of information security behaviors among citizens, consumers, and employees. To enhance the effectiveness of cybersecurity programs, addressing these challenges from a psychological perspective is essential. Understanding how individuals perceive cyber risks is paramount and necessitates effective awareness campaigns.

These campaigns should aim to foster comprehension and adherence to the advice of cybersecurity professionals, thereby cultivating a desire to change behaviors and intentions among internet users. This approach goes beyond merely providing information about cyber risks, employing persuasion techniques such as "fear appeals," which are widely used in cybersecurity awareness development studies (Tosun et al., 2020).

Additionally, the findings and recommendations of several previous studies have underscored the importance of cybersecurity and the necessity of educating internet users to protect their data and maintain a secure environment free from hacking, espionage, and blackmail. Notable studies in this regard include those by Al-Muntashari and Hariri (2020), Al-Qaisi (2020), Ibrahim (2021), Richardson et al. (2020), Sayegh (2018), and Al-Qahtani ,2018).

Recently, researchers at the Western level have focused on the proliferation of training programs aimed at enhancing cybersecurity awareness. These programs aim to identify key factors that contribute to achieving cybersecurity or its failure. Successful implementation can lead to behavioral changes among users, improving their security practices. Noteworthy studies in this area include those by Proctor (2016), Banfield (2016), and Chang & Coppel.(2020)

Although there is considerable interest in specialized scientific journals regarding training and outreach programs aimed at enhancing cybersecurity awareness, relatively little attention has been directed towards local and Arab studies in this field.

In recognizing the significance of this issue, the importance of fostering cybersecurity awareness among the primary demographic using the internet, specifically teenagers, becomes evident. However, studies focusing on samples of teenagers within the Arab and local communities are scarce, as far as current knowledge extends. The fundamental question addressed by the two researchers in this study revolves around assessing the effectiveness of a guidance program aimed at enhancing cybersecurity awareness among secondary school students in Riyadh.

Therefore, the researchers propose to investigate the effectiveness of a counselling program in enhancing cyber security awareness among secondary school students in Riyadh Region's who use the internet. The study is based on the following hypotheses:

H0.1: There are statistically significant differences in the average scores of the experimental group on the pre- and post-scale cyber security awareness test following the counselling program.

H0.2: There are no statistically significant differences in the average scores of the experimental group members and the control group members on the cyber security awareness scale after implementing the counselling program**.**

H0.3: There are no statistically significant differences in the average scores of the experimental group members on the cyber security awareness test between the post-program assessment and the follow-up assessment (one month later) after implementing the counselling program**.**

The study's objectives

The current study aims to:

1-Evaluate the effectiveness of a counselling program in enhancing cyber security awareness among adolescent secondary school students in Riyadh.

2- Assess the sustained effectiveness of the proposed counselling program in developing cyber security awareness among adolescent secondary school students in Riyadh schools one month after program implementation.

.

Table 1 ***experimental design***

Groups	-test	Independent variable(**Couns elling** program)	-test	Repeated- - - test
Experimental	Pre-test	Not applied program	Post- test	There is No Repeated- Scale
Control	Pre-test		Post-test	

Methodology:

A semi-experimental approach was adopted.

Sample :

The study included two samples:

A) Exploratory Sample: *This sample comprised 109 adolescents from the third year of secondary school in schools located in city, with an average age of 18.5 years. This sample was selected to assess the psychometric properties of the cyber security awareness scale. The schools from which participants were drawn are detailed in the following table.*

B) Counselling Intervention Sample: *This sample consisted of participants who met the study's inclusion criteria, which included regular students in their third year of secondary school and those who had scored low on the cyber security awareness test. The intervention sample used for the counselling program included 30 individuals, comprising 15 students in the experimental group and 15 in the control group...*

Data Collection Tools:

The Cyber Security Awareness Scale, developed by Noura Al-Sanea and colleagues (2020), consists of 30 items organized into two dimensions. The first dimension assesses awareness of the concept of cyber security with 7 items, while the second dimension covers methods for maintaining information security with 23 items. The scale retains its original structure and has demonstrated strong psychometric properties, including reliability and validity. Validity was confirmed through face validity and internal consistency during its development by the authors.

Regarding reliability, the Cyber Security Awareness Scale was assessed using Cronbach's alpha coefficient, which yielded a value of 0.91, indicating high internal consistency. The scale employs a five-point Likert-type response format with options ranging from "completely applies" to "does not apply completely," scored from 1 to 5.

Counselling Program:

The program is operationally defined as a structured set of instructions, information, experiences, and relevant skills delivered within a specific framework. Its purpose is to enhance cyber security awareness and equip individuals with the necessary skills and experiences to navigate this domain effectively.

The Goal of the Program :

This program aims to foster cyber security awareness among teenagers, with multiple objectives. It seeks to impart a comprehensive understanding of cyber security and its significance, educate teenagers about various cyber threats, and teach methods for safeguarding information on computers.

Statistical analysis was performed using SPSS version 24. The Mann–Whitney test was employed to evaluate the first and second hypotheses, while the Wilcoxon signed-rank test was utilized to assess the third hypothesis**.**

The Study's Variables :

The study investigates if a cybersecurity counselling program (independent variable) increases awareness of cybersecurity (dependent variable).

Results:

The Effectiveness of a Counselling Program in Enhancing Cybersecurity Awareness

Statistically significant differences were observed in the average scores of the experimental group on the cybersecurity awareness test between the pre- and post-intervention assessments. The Wilcoxon Signed Ranks Test was employed to evaluate these differences, and the results are presented in Table 2.

According to Table 2, there were statistically significant differences at the 0.001 significance level between the pre- and post-intervention scores on the cybersecurity awareness test. These differences favored the post-intervention assessment, indicating the effectiveness of the counselling program.

Table 2. The results of Wilcoxon Signed-Rank test for *awareness* of *cyber security*. in the experimental group

dimensions of ***Cyber security Awareness*** Scale		N	Mean Rank	Sum of Ranks	*Z*	*P*
Awareness of the concept of cyber security	Negative Ranks	9	6.89	62.00	-2.585	.010
	Positive Ranks	2	2.00	4.00		
	Ties	4c				
	Total	15				.001
Ways to keep information secure	*Negative Ranks*	*0a*	*.00*	*.00*	- 3.414-	
	Positive Ranks	*15b*	*8.00*	*120.00*		
	Ties	*0c*				
	Total	*15*				

Comparison of Cybersecurity Awareness Between Experimental and Control Groups

No statistically significant differences were found in the ranks of the average scores between the experimental and control groups on the cybersecurity awareness scale following the implementation of the counselling program. The Mann-Whitney Test was conducted to evaluate this hypothesis, and the results are presented in Table 3.

According to Table 3, statistically significant differences were observed at the 0.001 significance level between the scores of the experimental and control groups on the cybersecurity awareness test after the application of the counselling program. These differences favored the experimental group, demonstrating the program's effectiveness.

.Table 3. Mann-Whitney U test pre-test results of *awareness* of *cyber security* in the control and the experimental group

dimensions of ***Cyber security Awareness*** Scale	Groups	N	Mean Rank	Sum of Ranks	**z**	***P***
Awareness of the concept of cyber security	Experimental Group	*15*	20.07	301.00	- 2.891-	.004
	Control Group	*15*	10.93	164.00		
	Total	*30*			-4.691	0.00
Ways to keep information secure	Experimental Group	*15*	8.00	120.00		
	Control Group	*15*	23.00	345.00		
	Total	*30*				

Sustained Effectiveness of the Counselling Program on Cybersecurity Awareness

No statistically significant differences were found in the average scores of the experimental group members on the cybersecurity awareness test between the post-intervention assessment and the follow-up assessment conducted one month later. The Wilcoxon Signed Ranks Test was used to evaluate this hypothesis, and the results are shown in Table 4.

Table 4 indicates that there are no statistically significant differences between the post-intervention and follow-up measurements in cybersecurity awareness across its various dimensions.

Table 4. The significant differences between Mean Rank using the Wilcoxon test to detect the differences between the post measurement and follow-up of the experimental group on *awareness* of *cyber security*

dimensions of ***Cyber security Awareness Scale***	Groups	N	Mean Rank	Sum of Ranks	***z***	***P***
Awareness of the concept of cyber security	Experimental sample posttest	5	3.50	17.50	**-1.633**	.102
	Experimental sample follow-up test	1	3.50	3.50		
	Total	9^c			**-.302**	0.763
Ways to keep information secure	Experimental sample posttest	15				
	Experimental sample follow-up test	5^d	4.00	20.00		
	Total	3^e	5.33	16.00		

Discussion:

The results of the first hypothesis reveal statistically significant differences at the 0.001 significance level between the pre- and post-intervention scores on the cybersecurity awareness test. Specifically, the post-intervention scores of the experimental group were significantly higher than their pre-intervention scores. This outcome aligns with the anticipated direction, indicating an improvement in cybersecurity awareness following the application of the counselling program.

This signifies an improvement in cybersecurity awareness among the experimental group members following the implementation of the counselling program. This result alone confirms the program's effectiveness in enhancing cybersecurity awareness. It suggests that the counselling program successfully provided the experimental group members with the opportunity to learn about cybersecurity.

The integrated activities in the current program related to information security have proven effective in enhancing protection and education about cybersecurity. This includes educational videos about cybersecurity dangers and threats, along with instructions for maintaining cybersecurity. The positive participation of students in the counselling program significantly contributed to their awareness of maintaining a safe electronic environment. By following the necessary procedures to secure information and continuously implementing these practices, students developed a greater understanding of cybersecurity.

This result aligns with Ibrahim's (2021) study, which found a statistically significant difference at the 0.05 level between the average scores of participants in the pre- and post-application of the awareness scale, favoring the post-application. Similarly, Metwally's (2021) study revealed a positive, statistically significant correlation between the frequency of exposure to cybersecurity videos on YouTube and the level of cybersecurity awareness among respondents.

The current findings are consistent with those of Bada and Surse (2020), which demonstrated the effectiveness of a training program in enhancing cybersecurity-related thinking and cultural practices. Similarly, Chang and Coppel (2020) found that a training program successfully increased cybersecurity awareness among bank employees. However, the current results contradict those of Banfield (2016), which found no significant impact of a cybersecurity awareness program on changing security behaviors among workers, and Proctor (2016), which concluded that a training program did not effectively develop cybersecurity awareness.

Regarding the second hypothesis, the results indicate statistically significant differences at the 0.001 significance level between the scores of the experimental and control groups on the cybersecurity awareness test following the implementation of the counselling program. Specifically, the scores of the experimental group members were higher than those of the control group. This outcome is attributed to the positive impact of the counselling program, which involved a series of structured, organized, and sequentially timed sessions. These sessions utilized various techniques such as lectures, discussions, dialogues, brainstorming, and workshops aimed at enhancing cybersecurity awareness.

Conversely, these techniques offered valuable opportunities and practical experiences that the experimental group members encountered during their participation in the program. They acquired essential practices for maintaining information security and understanding various cyber threats. Active engagement characterized their involvement in the counselling sessions, where they not only received information but also actively practiced and interacted in a scholarly manner under the researcher's supervision and guidance.

. This finding aligns with several studies, such as Bicak et al. (2015), which identified differences in cybersecurity levels between control and experimental groups of graduate students. Similarly, it corresponds with the conclusions of Li et al. (2020), which demonstrated the effectiveness of a program utilizing non-formal education and educational portfolios in enhancing cybersecurity awareness.

Regarding the discussion of the results from the third hypothesis, which showed no statistically significant differences between the post-intervention and follow-up measurements in cybersecurity awareness across its various dimensions, this suggests that the program's impact persists in developing cybersecurity awareness among the members of the experimental group. Importantly, this effect was sustained between the immediate post-intervention assessment and the follow-up evaluation.

The techniques employed in the counselling program among the experimental group members contributed to enhancing their cybersecurity awareness. This program utilized methods such as dialogue, discussion, lectures, and videos across multiple sessions.

The sustained development of cybersecurity awareness among the experimental group can be attributed to the program's content, which covered topics such as cyber threats, information security practices, methods for preventing hacking, and understanding legal regulations related to cybercrimes and hacking. This comprehensive approach has significantly contributed to enhancing cybersecurity awareness within the experimental group.

Conversely, the sustained effectiveness of the program can be attributed to the researcher's role as a role model for students, fostering an environment characterized by friendliness, affection, familiarity, and enjoyment. Throughout the sessions, the researcher aimed to cultivate this atmosphere, which has contributed to the program's ongoing effectiveness.

One month after applying it to the experimental group. .In addition, this result is supported by what was indicated by the results of the studies of Al-Muntashari and Hariri 2020, Al-Qahtani 2019, Al-Sahafi and Askoul 2019, , Sayegh 2018).

The results of the first hypothesis indicate that there are statistically significant differences at the level of significance (0.001) between the scores of the pre- and post-measurements on the cyber security awareness test after applying the guidance program in the direction of the post-measurement: meaning that the scores of the experimental group members in the post-measurement on the cyber security awareness test were higher. From the pre-measurement scores of the same group, this result came in the expected direction.

This represents an improvement in the level of awareness of cyber security among the members of the experimental group after implementing the guidance program. This result confirms - on its own - the effectiveness of the guidance program, and that it leads to improving the level of awareness of cyber security. This result can be interpreted that the guidance program has provided the opportunity The members of the experimental group have the opportunity to learn about cyber security.

Through the integrated activities provided in the current program related to information security; It enhances protection and education about cyber security, as well as providing educational videos about the dangers and threats of cyber security, and providing instructions for maintaining cyber security. The positive participation of students in the guidance program was also evident in developing their awareness of maintaining a safe electronic environment, by following the necessary procedures to secure information, and working to implement This is to work continuously, and this result was consistent with the results of Ibrahim's study (2021).

Which resulted in a statistically significant difference at the level (0.05) between the average scores of the parameters in the pre- and post-applications of the awareness scale. In favor of post-application; And with the results of Metwally's study (2021), which revealed the existence of a positive, statistically significant correlation between the rate of exposure of respondents to cyber security videos on YouTube, and their level of cyber security awareness.

The current result is consistent with the results of the study (Bada & Surse, 2020), which revealed the effectiveness of a training program in enhancing practices related to thinking and culture related to cyber security, and with the results of the study (Chang & Coppel, 2020), which revealed the ability of a training program; To enhance cyber security awareness among bank workers. On the other hand, the current result contradicts the results of the study (Banfield, 2016), which revealed that there is no significant effect of implementing a cyber security awareness program in changing security behaviors among workers. With the results of the study (Proctor, 2016), which concluded that the effectiveness of a training program for developing cyber security awareness was not achieved.

Regarding the second hypothesis, its results show that there are statistically significant differences at the level of significance (0.001) between the scores of the experimental and control groups on the cyber security awareness test after applying the guidance program in the direction of the experimental group: meaning that the scores of the experimental group members on the cyber security awareness test were higher than the control group's scores. We attribute this result to the positive impact of the counselling program based on a group of planned, organized, and time-sequential sessions, mediated by the use of several techniques; With the aim of developing awareness of cyber security, these techniques include: lecture, discussion, dialogue, brainstorming, and workshop.

On the other hand, these techniques provided appropriate opportunities and live experiences that the experimental group members lived throughout their attendance in the program, and they acquired a set of practices that were necessary to maintain information security and awareness of various cyber threats. The experimental group members also actively participated in the counselling sessions, so they were not only recipients, but they also practiced and interacted directly through scientific performance under the supervision and guidance of the researcher.

This result is consistent with many studies: including the study (Bicak et al., 2015), which concluded that there are differences between the control and experimental group of graduate students in the level of cyber security. This result is consistent with the results of the study (Li et al., 2020), which concluded To the effectiveness of a program based on non-formal education and portfolios Educational in developing awareness of cyber security.

As for discussing the results of the third hypothesis, which indicated that there were no statistically significant differences between the post and follow-up measurements in awareness of cyber security in its various dimensions, this indicates that the program's effect remains in developing awareness of cyber security among members of the experimental group and that this effect does not disappear between the two post and follow-up applications.

It can be said that the techniques of the guidance program among the experimental group members contributed to developing their awareness of cyber security. Through the guidance program based on the techniques of dialogue, discussion, lecture and video in various sessions.

The continued impact of the program in developing awareness of cyber security among the experimental group is due to the content of the program in which they were trained, and the information it included regarding cyber threats, how to maintain information security, ways to prevent hacking, and knowledge of legal legislation for cybercrimes and hackings. All of this has contributed to the development of Awareness of cyber security among the experimental group.

Furthermore, the sustained effectiveness of the program is attributed to the researcher's role as a model for students, fostering an environment characterized by friendliness, affection, familiarity, and enjoyment. This supportive atmosphere was maintained throughout the sessions, contributing to the program's continued effectiveness one month after its implementation with the experimental group.

Moreover, this finding is corroborated by the results of studies conducted by Al-Muntashari and Hariri (2020), Al-Qahtani (2019), Al-Sahafi and Askoul (2019), and Sayegh(2018).

***Recommendations*:**

In light of the current results, the study recommends the following:

1-Activating the role of guidance and training programs that aim to develop awareness of the principles of dealing with the Internet, social networking sites and the dangers of the Internet for different age groups of its users.

2-Integrating cyber security into curricula in schools and universities.

3-Increasing psychological research and studies on psychological factors (cognitive and mood) and clarifying their role in maintaining the security of cyber information .

4- Conducting courses for cyber security personnel on raising awareness of the human factors responsible for an individual's cyber threats, as well as the human factors behind not maintaining information security.

5-Awareness and training programs in the field of cyber security can be part of national security, and must be well organized to provide people with basic knowledge of cyber security, by focusing on educational environments and periodically analyzing the security awareness of Internet users, mediated by a comprehensive plan for security awareness and training.

Acknowledgments:

Special thanks are extended to both the psychological counsellors and the students who contributed to the experiment. Their participation and support were invaluable to the study's success.

Funding sources.

Deanship of Scientific Research. Imam Muhammad Bin Saud Islamic University. Riyadh. Saudi Arabia (IMSIU)

References

Ahram, T., & Karwowski, W. (Eds.). (2019). Advances in Human Factors in Cyber security: Proceedings of the AHFE 2019 International Conference on Human Factors in Cyber security, July 24-28, 2019, Washington DC, USA (Vol. 960).

Springer. Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3) , 2-16.

Al-Dhuwaifiri, M. (2021), The reality of cyber security and increasing its effectiveness in public education in the Medina region from the point of view of school leadership. International Journal of Educational and Psychological Studies. 10, (3), 635-655. Al-Manea, J. (2022). Requirements for achieving cyber security in Saudi universities in light of Vision 2030. College of Education Journal. Assiut University. 4, (38), .155-194.

Al-Montashri, F., & Hariri, R. (2020) The degree of middle school teachers' awareness of cybersecurity in public schools in Jeddah from the teachers' point of view. Arab Journal of Specific Education. Arab Foundation for Education, Science and Arts, 14(1) 95-140.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. International Journal for Information Security Research (IJISR), 6(2), 660-666.

Al-Qahtani, N. (2019). The extent of awareness of cyber security among male and female students at Saudi universities from a social perspective: a field study, Social Affairs Journal. 85-120.

Al-Qaisi, M., (2020) The future of global strategic security in light of the challenges of technology - information and cyberspace. Journal of Regional Studies. University of Mosul, Center for Regional Studies (44)13, 139–-173. .

Al-Ruwais, F , A. (2013). The social effects of Internet addiction: A field study on a sample of male and female third-year secondary school students in Afif Governorate. Journal of the Service Center for Research Consultations.(47). 128-168.

Alsahfy ,M & Al-Askoul, S, (2019) The level of cyber security awareness among secondary school computer teachers in Jeddah. Journal of Scientific Research in Education, Girls’ College of Arts, Sciences and Education. Ain Shams University, 20(10), 493-534.

Al-Sanea, N (2020.) Teachers’ awareness of cyber security and ways to protect students from Internet risks and enhance their national values and identity. Journal of the Faculty of Education: Assiut University - Faculty of Education,36.(6).41-57.

Al-Sanea, N, Omar; A, Awatif, S Al-Din; Al-Sawat H ,Abu Aisha, Z; Suleiman, E, (2020). Teachers’ awareness of cyber security and ways to protect students from Internet risks and enhance their national values and identity. Journal of Scientific Research in Education, vol. 36,. (6), 41-90. .

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), 1-13.

Bada, M., & Nurse, J. R. (2020). The social & psychological impact of cyber attacks. In Emerging cyber threats & cognitive vulnerabilities (pp. 73-92). Academic Press.

Bada, M., & Nurse, J. R. C. (2019). Developing cyber security education and awareness programmers for small-and medium-sized enterprises (SMEs). Information and Computer Security, 27 (3), 393–410.

Banfield, J. M. (2016). A study of information security awareness program effectiveness in predicting end-user security behavior. Eastern Michigan University.

Bicak, A., Liu, X. M., & Murphy, D. (2015). Cyber security curriculum development: introducing specialties in a graduate program. Information Systems Education Journal, 13(3), 99-110.

Bordoff, S., Chen, Q., & Yan, Z. (2017). Cyber attacks, contributing factors, and tackling strategies: the current status of the science of cyber security. International Journal of Cyber Behavior, Psychology and Learning, 7(4), 68-82.

Cash, S. J., Thelwall, M., Peck, S. N., Ferrell, J. Z., & Bridge, J. A. (2013). Adolescent suicide statements on MySpace. Cyber psychology, Behavior, and Social Networking. 16(3), 166-174.

Chang, L. Y., & Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from Myanmar. Computers & Security, 97,(2). 1-10.

Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. Revista de Administrative Publica si Politici Sociale, 12(1), 40. 120-136.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., & Huettel, S. A. (2014). An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt. impulsiveness scale version 11. Archives of scientific psychology, 2(1), 1-12.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber security. Technology Innovation Management Review. 4(10):13-21.

Faramawi, M. (1992). Educational planning programs. Anglo-Egyptian Library. Cairo

Gcaza, N., & Von Solms, R. (2017). A strategy for a cyber security culture: A South African perspective. The Electronic Journal of Information Systems in Developing Countries, 80(1), 1-17.

Hadlington, L., & Parsons, K. (2017). Can cyber loafing and Internet addiction affect organizational information security?. Cyber psychology, Behavior, and Social Networking, 20(9).567-571. ,

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. . Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016, November). Cultural and psychological factors in cyber-security. In Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services (pp. 318-324) .

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of information systems, 18, 106-125.

Ibrahim, M., H (2021) Awareness of cyber security aspects in distance education. Scientific Journal of King Faisal University. administration science. Mug 22..(2). 299-307.

Kaloudi, N., & Li, J. (2020). The air-based cyber threat landscape: A survey. ACM Computing Surveys, 53(1), 1-34.

Khalifa, I (2017), “Growing cyber threats to military institutions”, Trends of Events Magazine,. 22, (July/August.) .

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267.

Li, J., Pang, M., Smith, J., Pawliuk, C., & Pike, I. (2020). In search of concrete outcomes—A systematic review on the effectiveness of educational interventions on reducing acute occupational injuries. International journal of environmental research and public health, 17(18), 6874.

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. Communications of the ACM, 63(12), 64-80.

Metwally, A. (2021). The role of YouTube in developing adolescents' awareness of electronic security. Middle East Public Relations Research Journal. (31). 349-389. .

National Cyber security Authority (2020) National Cyber security Strategy. Kingdom of Saudi Arabia. sa.gov.nca. .

Odemis, M., Yucel, C., & Koltuksuz, A. (2022). Detecting User behavior in cyber threat intelligence: development of Honeypsy system. Security & Communication Networks, (22), Article ID 7620125, 28 pages1155-1072.

Parsons, K., McCormac, A., Pattinson, M., Jerram, C., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?. Information Management & Computer Security, 20(1), 18-28.

Proctor, W. R. (2016). Investigating the efficacy of cybersecurity awareness training programs (Doctoral dissertation,) Capstone Project Submitted to the Faculty of Utica College.

Raineri, E. M., & Resig, J. (2020). Evaluating Self-Efficacy Pertaining to Cyber security for Small Businesses. Journal of Applied Business & Economics, 22(12). 13-23 .

Richardson, M., MacDowall, W., Burchett, H., Stansfield, C., ... & Thomas, J. (2020). Cyberbullying and children and young people's mental health: a systematic map of systematic reviews. Cyber psychology, Behavior, and Social Networking, 23(2), 72-82.

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cyber security training model to support an organizational awareness program: The Cyber security Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology 21(3), 26-39.

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cyber security training model to support an organizational awareness program: The Cyber security Awareness TRAining Model (CATRAM). A Case Study in Canada. In Research Anthology on Artificial Intelligence Applications in Security (pp. 174-188). IGI Global.

Sayegh, W. (2018) Family members' awareness of the concept of cyber security and its relationship to their security precautions against cybercrimes, Arab Journal of Social Sciences, Arab Foundation for Scientific Consultation and Human Resources Development. 3 (14) 18-70. .

Seigfried-Spellar, K. C., Flores, B. M., & Griffin, D. J. (2015, October). Explanatory Case Study of the Authur Pendragon Cyber Threat: Socio-psychological & Communication Perspectives. In International Conference on Digital Forensics & Cyber Crime (pp. 143-175).

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cyber security behavior. Psychology of Popular Media, 9(4), 475–480.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100.

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

Taha, F., Abdel Fattah, M., Mohamed, H., & Qandil, S. (2003), Encyclopedia of Psychology and Psychoanalysis, 2nd ed. Strange house. :Cairo. .

Tosun, N., Altinöz, M., Çay, E., Çinkiliç, T., Gülseçen, S., Yildirim, T., ... & Ünlü, N. (2020). A swot analysis to raise awareness about cyber security & proper use of social media: Istanbul sample. International Journal of Curriculum & Instruction, 12, 271-294.

Waasdorp, T. E., & Bradshaw, C. P. (2015). The overlap between cyberbullying and traditional bullying. Journal of adolescent health, 56(5), 483-488.

Wiederhold, B. K., Gao, K., Sulea, C., & Wiederhold, M. D. (2014). Virtual reality as a distraction technique in chronic pain patients. Cyber psychology, Behavior, and Social Networking, 17(6), 346-352 .

Younis, Y. A., Shi, Q., & Askwith, B Topham, L., Kifayat, K.,. (2016). Cyber security teaching and learning laboratories: A survey. Information & Security, 35(1), 51-71