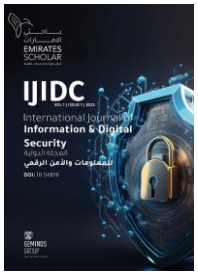

International Journal of Information & Digital Security
Vol 1 Issue 1 (2023)
Pages (20 –31)

Available at www.emiratesscholar.com

The Necessity of Cybersecurity for Community Safety the Proposal of the Safe Family Program for Educating the Gulf Arab Community on Information Security for Both Students and Parents

Nabih Abdelmajid

Higher Colleges of Technology (HCT)

Abstract

The contemporary landscape of electronic communication technologies is marked by rapid advancement, diverse modalities, and intuitive interfaces, rendering them widely accessible across demographic strata. Notably, the youth cohort, including school students, exhibits a discernible proclivity towards the utilization of social media networks. Regrettably, this escalating adoption lacks the concomitant implementation of requisite competencies for judicious technological engagement. Furthermore, a perceptible dearth of cognizance is observed among students regarding the gravity of information security and the attendant repercussions of its neglect. This lacuna has precipitated a proliferation of cybersecurity issues, including hacking and electronic coercion. Despite instances of adept technological acumen among some students, they remain susceptible to exploitation by cyber adversaries. This discourse underscores the imperative for comprehensive educational initiatives aimed at fostering responsible and secure digital practices among the burgeoning generation of technology users.

This study conducted a survey among diverse groups of male and female students in the Kingdom of Saudi Arabia to identify the primary issues leading to their vulnerability to cyber intrusions. The objective was to derive necessary recommendations for their protection while engaging in social network activities. The study elucidated the importance of educating students about the ramifications of unsafe technology use, emphasizing the preservation of their electronic privacy.

Furthermore, this study addressed the exploration of the role of parents in safeguarding their offspring from the perils of cyber intrusion and extortion. The study conducted a comparative analysis between numerous families wherein parents and children had the opportunity for appropriate training in the use of these technologies and those families lacking such training. This comparative approach aimed to elucidate the role of parents in shielding their children from electronic intrusions. The findings of the study underscored a critically significant role for parents in protecting their children from electronic threats, even in cases where the offspring possessed a sufficient educational background in handling these new technologies.

The researcher proposed an educational initiative aimed at preserving electronic privacy for students, encompassing all categories of public and private education. In addition, a program for parental education was introduced, targeting both mothers and fathers. The objective of this program is to contribute to the elevation of societal security awareness and the protection of children from the imminent dangers posed by electronic threats.

Email address: Nabdelmajid@hct.ac.ae (Nabih Abdelmajid)

1. Introduction:

The domain of information security has held significant prominence since medieval times and continues to do so in contemporary society. The preservation of data confidentiality has emerged as a major concern for various societal segments, particularly state-affiliated institutions, entrusted with highly sensitive information. The advent of modern communication technologies, including computers and versatile smart devices, has intensified these concerns. The rapid transition to internet use and the communications revolution in various aspects of life have exacerbated the challenge, leading to an unprecedented surge in interest and adoption among diverse societal groups.

Despite the advantages of increased efficiency and productivity resulting from rapid advancements in communication technologies, there is a severe and unfortunate downside: the creation of numerous technical issues. The root cause of these problems and their escalation lies in the lack of prior qualification for users before engaging in this technological unknown. The precipitous increase in the adoption of these modern technological revolutions, particularly by inadequately qualified communities, has given rise to a plethora of security lapses and improper behaviors, rendering these communities susceptible to ill-intentioned actors commonly known as technology hackers.

The observable increase in cyber intrusions, privacy violations, extortion, and even manipulation of users' thoughts and beliefs poses a substantial danger to societies on various fronts. This has prompted significant interest and responsibility among researchers to enhance security protocols and ensure secure communication lines for users amidst this rapid technological evolution. Despite the presence of specialized protocols for secure data transmission, experts have struggled to attain a sufficient level of secure data exchange.

Study Problem:

Recent studies underscore the fundamental issue in our societies, namely the cognitive unreadiness of users to cope with the escalating cognitive cyber-attacks. Users have become susceptible to various forms of violations by malicious entities, including data breaches, online corruption through the dissemination of explicit content, financial theft, and extortion. Moreover, these intrusions extend to intellectual corruption and the propagation of misleading ideas, impacting a broad sector of the emerging youth population.

Study Questions

The study is divided into two distinct sets of questions, addressing specific inquiries aimed at uncovering the impact of social media usage on electronic privacy loss for users, along with the genuine reasons contributing to this phenomenon. The questions are outlined as follows:

Section A: Questions related to the Impact of Social Media Usage

2. **What is the level of enthusiasm for using various types of social media?**

3. **What are the objectives of students in using social media platforms?**

4. **What is the extent of exposure to security breaches and electronic extortion attempts?**

4. What is the cognitive awareness level regarding the risks associated with dealing with social media platforms?

Section B: Questions related to the Role of Parents in Protecting Children from Online Threats

5. **What is the knowledge level of parents in dealing with modern communication technologies?**

2. To what extent are parents aware of the dangers of unsafe interactions with these technologies?

6. **How invested are parents in monitoring their children's electronic transactions?**

4. What is the role of parents in shielding their children from falling prey to hackers?

5. Is training children to an excellent level of understanding modern communication technologies deemed sufficient for protecting them from the danger of electronic extortion?

These questions aim to explore the various dimensions of social media usage and its impact on privacy, as well as the role of parents in safeguarding their children from potential online threats.

Study Objectives:

The study objectives are divided into the following:

A. Understanding the Real Causes Behind the Hacker's Ability to Penetrate this Vital Segment, Which Constitutes the Foundation of Future Societies:

This part of the study aims to answer the questions posed in the preceding paragraph, seeking to provide recommendations that can mitigate breaches resulting from the misuse of social media platforms.

6.1. Recognizing the Role of Parents in Protecting Their Children from Hacking and Electronic Extortion:

This study aims to uncover the awareness level of parents regarding the dangers of modern communication technologies. It seeks to explore their knowledge and concern about the risks associated with these technologies. Furthermore, the study aims to reveal the truth about the role of parents and the importance of their involvement in achieving a stage of a secure family. This will be accomplished by addressing the questions posed in the second section of the inquiries

Importance of the Study:

Communities, with their diverse cultures and geographical locations, are universally exposed to the threats of hacking and electronic extortion. It is observed that this threat has encompassed all societal strata, as there have been recent infiltrations

into numerous official systems in multiple countries, causing significant damage to various institutions on various levels. Examples include entities like "SHEMOON1," "I WANA CRY," "SHEMOON2," and so forth. Additionally, there has been notable targeting of children, with a rise in attempts to export them in recent times. The reasons for this will be explored in this study.

Therefore, the importance of this study lies in understanding the real qualification level of male and female students in the field of modern communication security. It also aims to recognize the cognitive level of parents. Undoubtedly, this will necessitate making necessary recommendations to enable users to keep up with the rapid acceleration in information technologies for the global internet and social networks. It is crucial to enhance the readiness of our children in line with this fast-paced technological advancement, especially in secure interactions with social media platforms. The following details elaborate on the significance of this study across various dimensions:

6.2. Social Awareness in the Field of Cybersecurity:

Providing relevant and contemporary information to contribute to community awareness and transition it to a qualitative stage of secure internet and electronic communication usage.

6.3. The Safe Generation:

Offering necessary recommendations for the category of school students in their early stages, with the goal of "creating" a safe generation. This will contribute to empowering the next generation to face and keep up with the challenges of this rapidly evolving electronic revolution.

6.4. Secure Circles and Institutions:

The creation of a safe generation will inevitably lead to building a resilient fortress for national security and its institutions against the intrusion of intrusive elements and criminals in this electronic revolution

Previous Studies:

This study addresses three main axes with the aim of assessing the knowledge level within the two primary segments of society: students on one hand and parents on the other. The first axis focuses on the cognitive level of students, while the second axis delves into the cognitive level of parents. In addi- tion to these two axes, the researcher deems it necessary to add a third axis, through which various local and regional educa- tional initiatives are presented. These initiatives aim to enhance the knowledge level of users. The following details provide a breakdown of these axes.

First Axis: Cognitive Level of Students

Numerous previous studies and experiments have focused on the cognitive level of students, a category considered one of the crucial pillars in the development of societies. These stud- ies have been conducted across diverse cultures. The following highlights some important studies in this axis.

In 2011, professors in statistics and mathematics, Kroger, Stein, Durden, and information systems expert Flordi1, emphasized the significance of cultural factors as a primary influencer of community awareness outcomes. They asserted that the human factor, comprising closely related dimensions of knowledge and behavior, plays a vital role in the field of information technology and communication security. Researchers utilized an information security vocabulary test to assess the awareness levels related to human dimensions of knowledge and behavior among university students in different regions of South Africa. The aim was to determine whether cultural differences among students impact information security awareness levels in information technology and communication. Results indicated that certain cultural factors, such as native language and the region where students grew up, have a tangible effect on information security awareness levels. These factors should be considered when planning information security awareness programs. Surprisingly, over half of the students (54%) did not understand the term "security incident." Particularly striking was the fact that concepts associated with social engineering were not well-known or understood by the students. Nearly half (47%) admitted not knowing the meaning of "social engineering." Responses also revealed a lack of understanding of concepts such as "phishing" by around 40%, and 64% claimed not to know the meaning of "pharming." The study, demonstrated how students perceive information technology and communication security and their feelings of information safety.

As evident from the previous figure, most students require a specialized awareness program in information security to shield them from the risks associated with these modern technologies. In another study conducted by researcher Mohamed Boujettif from the University of Liverpool [2], a general survey was conducted on the awareness levels of 116 employees in 22 companies in information security within the Kingdom of Saudi Arabia in 2010. When questioned about their behaviors regarding their work, important data, computing habits, and other behaviors, the following findings emerged:

1. 83% did not have a backup copy of their work files.
2. 65% could easily guess passwords.
3. 78% did not update their computer systems with the latest updates.

These results raised significant concerns about the real deficiency in training within the companies included in the study. The findings also indicate that employees face other problems with their information systems in general, in addition to the security issues. The researcher found that the level of information security awareness among employees was very low. Here are some results indicating the low cognitive level of the employees:

1. 65% were not aware of current viruses
2. 60% felt they were vulnerable to attacks by hackers.
3. 65% either never used protective software or did not know how to use it.
4. 92% had never used anti-spyware programs.
5. 62% did not know the meaning of phishing.

The researcher noted that, despite some expressing significant interest in combating electronic crimes and avoiding hacking attempts:

1. 63% felt somewhat prepared to counter hacking attempts,

while 37% felt entirely unprepared.

2. Only 62% were cautious when opening email messages.

Through these various readings, the researcher concluded that the community needs a training program aimed at raising the electronic security awareness of employees. In a study by researcher Aliaa Ahmed Aldosari [3] from the International Islamic University in Malaysia, a study was conducted on the Saudi community to assess the awareness level of security threats based on their knowledge, behavior, and culture. The researcher selected students from two universities in the eastern region of Saudi Arabia. The study revealed the impact of students' knowledge on their behavior regarding security risks, especially those personally related to them, such as email attachments, spam emails, and pirated software. The study concluded that students who received specialized information security training have a better ability to prevent many security problems they may encounter. Researchers Oksanen and Kibble [4] intentionally conducted a cross-sectional survey in their study on the Finnish community. They relied on data collected about the population regarding their exposure to cybercrimes aged between 15 and 74 years. The number of cases analyzed reached 46,139. The analysis of this data showed that the youngest age group (15 to 24 years) is the most exposed to cybercrimes compared to older age groups. Despite the various study factors related to the youth category, such as gender, education, and economic status, the youth category remained the most exposed to falling victim to hackers. The findings of this study indicated that social violence exercised by the age group between 15 and 24 years is associated with the degree of exposure to harm from cybercrimes. The study also revealed that good social networks acted as a preventive measure against harm from cybercrimes among females. This study demonstrated that the leniency towards the dangers of modern digital communications may lead to disturbing the thoughts of young people, contributing to increasing violence and exposing them to significant psychological risks.

umber "1": Level of Knowledge of Male and Female Students Regarding Types of Viruses [4]

In a distinctive work by a group of researchers from the University of Plymouth in the UK, during an investigative research study, it was pointed out that initiatives and programs aimed at raising awareness of electronic information security are predominantly directed towards organizations and institutions, neglecting home users. The researchers aimed to address several important issues in their study, particularly assessing the level of awareness in information security and its practical application. The study indicated that most of the study sample is not familiar with new types of cyber threats, as illustrated in Table 1, exposing them to various electronic breaches. Consequently, the study concluded on the necessity of educating users on how to use modern communication technology, positively impacting users' ability to protect their electronic privacy. The study also highlighted that trained users exhibit a high level of security awareness, while the untrained category remains at a lower security level.

"Morphard," "Keigenberg," and "CrossClags 6" are a group of researchers in the United States who believe that cybercrimes can cause multiple damages to users, especially university students, due to their extensive use of internet technology and modern digital communications. Consequently, these researchers conducted a study to examine the impact of cybercrimes on these students. The researchers conducted 10 interviews as a basis for constructing a specialized questionnaire to understand the students' knowledge, perceptions, and behaviors regarding cybercrimes. They found that over 50% of well-connected students using modern communication technologies had experienced at least one case of electronic intrusion involving malicious software, piracy, or phishing. Furthermore, the researchers indicated that students primarily rely on the experiences of individuals who have fallen victim to hackers as their source of information. Despite the ease of access to cybercrime statistics, the researchers discovered that the majority of students do not formally report electronic crimes. They also identified that 34% of the crimes against students involved malware, 20% were related to electronic piracy, and 19% were phishing scams. Given the relatively high prevalence of these rates, the researchers emphasized the need for practical and awareness training to elevate students' knowledge about information security and empower them to safeguard their privacy, even in highly cultured and aware societies like the United States.

Researcher "Stephanie Markham" emphasizes the necessity of incorporating information security into all university curricula due to its critical need for all students. The researcher argues against restricting the teaching of information security topics solely to Computer Science (CS) or Computer Information Systems (CIS) students. Instead, the researcher suggests that the need for global communication enhances the necessity for security across all fields. In her study, the researcher describes proposed methods to integrate information security into curricula across various disciplines through the implementation of real-world scenarios and relevant exercises. Similar findings were reached by "North" and "George" through an investigative study on computer science and other specializations. They indicated that scientific specializations in computer science exhibited a higher awareness of information security and its ethics compared to other specializations. Based on these results, the researchers presented brief recommendations:

1. Provide specialized modules for computer security courses that offer fundamental information about computers, security, and ethics.
2. Develop training courses to teach university students about installing antivirus programs and firewalls.
3. Establish a dedicated section for students on the university's website to access the latest information and updates on relevant software and issues.
4. Organize workshops or presentations with technical speakers currently working in the field of information security to provide up-to-date information on computer security, ethics, and the necessary awareness.

Researchers "Grose" and "Rossow" conducted a survey involving a wide range of internet users and modern communication technology enthusiasts. They found that users struggle

Virus Type	I Know	I don't Know
Virus/Worm	92	0
Trojan Hourse	80	3
Spam	90	0
Social Engendering	44	24
Phishing	70	10
Pharming	24	42
Identity Theft	81	18
Key Loggers	57	22
Phloppinga	7	68
Botnets	7	68
Zombies	33	38
Denial of service	56	24
Packet sniffer	47	37
Whoopinga	10	59
Hacker	95	1
Zero day attacks	29	44
Cracker	56	24

Figure 1:

to differentiate between security issues and computer-related problems, causing continuous and persistent security concerns. As a result, the researchers recommend broad-scale training to alleviate this sense of anxiety and empower users to face these risks.

In another study by researcher Abdulaziz, along with colleagues "Hayland" and "Twuttle" from the University of Wollongong in Australia, they confirmed that awareness of security threats is increasing in the Western world but is decreasing in regions like Saudi Arabia. Therefore, the researcher studied the level of information security awareness among the general population in Saudi Arabia using an online survey with 633 participants. The results indicated very low levels of awareness, illustrated by the following examples:

1. Only 29% of 462 respondents indicated that they always keep their mobile devices in secure places, while 43.1% keep them secure some of the time, and 22.7% do not keep their devices secure at all.

2. Approximately 55.2% use a password to access their devices, while 39.7% do not use any password.

3. A high percentage (65.7%) do not change their passwords periodically.

4. 45% choose weak passwords.

5. 35.8% share their passwords with their families.

6. Only 7.4% are aware of Denial-of-Service issues.

7. About 14% use intrusion detection programs, and 53% have not updated their protection software in over three months.

8. Approximately 44% do not back up their files.

9. 80.5% do not know how or where to report security incidents.

These combined percentages indicate a very low level of awareness in the Saudi Arabian community. Such low awareness can lead to significant security breaches, potentially causing substantial harm to the kingdom’s security. In the sec-

ond axis, the researcher presents studies on understanding the knowledge level of parents and the importance of their role in protecting families and society.

Second Axis: The Cognitive Level of Parents and the Importance of Their Role in Protecting Their Children

Before delving into the cognitive level of parents, the researcher first addressed the discussions regarding the degree of interest and inclination of children towards using the Internet and social media in diverse societies and cultures. This is of significant importance, placing the responsibility on parents to keep up with their children. A European survey mentioned in the study indicated that 96% of European children use the Internet regularly. Another study focusing on the Swedish society revealed that over 90% of families and their children use the Internet. In Turkey, a study showed a similar enthusiasm, with the majority of children using the Internet from various loca- tions such as home, internet cafes, school, library, and during visits to friends. In the United States, the majority of children under 18 years old are Internet users, and a study found that most of them have personal computers at home.

The next part of the study is dedicated to exploring the high level of interest among students in Saudi society and investigating the cognitive level of this group.

Regarding parents, multiple studies have examined the importance of the role of parents in protecting their children from the dangers of the Internet and modern digital communication technologies. These studies covered various societies to assess the cognitive level of parents and the extent of their concerns and fears regarding the impact of the Internet on their children.

Researcher Samir Hamad from Kuwait pointed out that the majority of parents have a moderate awareness of their children's online activities, and this level of awareness is insufficient for monitoring their children effectively. The researcher found that only 12% of parents have a moderate level of monitoring their children's Internet usage. As Internet use by children increases, parents express significant concern about the potential negative values that may influence their children. Many parents are uncomfortable with the content their children may access on the Internet, including explicit material, and they are not ruling out the possibility of their children encountering sexually explicit content or being exposed to attempts at extortion.

Several statistical studies conducted by researchers like Kapsi, Odabas, Koklar, Mich, Ponti, and Symois have delved into these aspects.

The study by "Eurobarometer 20" stands out, where the researcher conducted an extensive study on parents' opinions regarding their children's Internet use. The study addressed various aspects, including:

1. Children's Internet and mobile phone usage and the degree of their connection with their parents.

7. **Concerns about the risks children face when using the Internet**

8. **Instances where children sought help from their parents regarding Internet-related problems**

4. Parental supervision (methods used for supervising their children's Internet usage and the level of skills employed).

5. Institutions or systems through which parents can report any illegal and harmful content observed during Internet use.

9. **Perspectives on measures that could contribute to safer Internet use for parents**

10. **Preferred sources for obtaining information and advice on safe Internet usage**

The study included families with children aged 16 to 19. Regarding the degree of interest, the researcher found that nine out of ten children use the Internet in European society. The percentage of children with mobile phones reached one-third compared to the 2005/2006 period when the percentage was only 48% for children aged 6 to 17. This indicates a significant increase in Internet use among children.

Regarding the concerns experienced by parents, 65% of them indicated that they believe their children are watching ex- plicit movies and visiting frightening websites. Additionally, 45% of these parents are very concerned about this. The study revealed that 60% of parents are worried about the possibility of their children being exposed to online solicitation, and 45% of families expressed fear that their children might be subjected to intimidation on the Internet. Around 50% of families believe that their children are exposed to electronic extortion. Furthermore, many parents pointed out that their children might disclose personal or private information while using the Internet. This study included various charts illustrating the high level of fear experienced by parents for their children in different forms of European society. This necessitates effective solutions from stakeholders in this sector to address such issues.

Regarding the strategies adopted by parents to protect their children from online dangers, three-quarters of parents mentioned that all they have is talking to their children about their online activities and sitting close to them when they use these technologies. Some parents also rely on family and friends for advice on protection tools, monitoring, filtering, and safe internet use. Approximately 71% of parents turn to a friend to discuss internet safety issues. However, these sources may not always be reliable and can lead to various problems, as they rely on scattered and non-specialized experiences.

In another study by researchers "Zaikar" and "Barkak" on the importance of parental roles, they indicated that most students have a very low level of knowledge regarding safe internet use. Given this low level of knowledge, the researchers emphasized the need for parents to invest more in educating their children to protect them from electronic risks. Additionally, they suggested that teachers should allocate more educational materials related

to the internet and its dangers and spend more time training and empowering students with skills to counter hacking attempts.

Concerning parents' fears for their children, some studies have shown that most parents try to check what their children are browsing on the internet and stay close to them to monitor the websites they visit. To achieve effective monitoring, parents need to be well-qualified. To uncover the role of parents in protecting their children, the researcher dedicated a specific part of this study to presenting a realistic study of several families in Saudi society, aiming to reveal the level of knowledge among parents and understand their actual role in protecting their children.

Axis Three: Information Security Initiatives

Numerous initiatives focused on information security have emerged in the region. These initiatives, from various sources, aim to raise awareness about information security within communities. The following is a study highlighting these initiatives, their positive aspects, and potential drawbacks:

1. **"Your Awareness Protects Us" Initiative:** This initiative was launched in the Kingdom of Saudi Arabia with the goal of enhancing electronic security awareness among the lo- cal community. It was implemented in response to Cabinet Decision No. 81 of the year 1430 H, which directed government entities to quickly develop informational programs on information security and implement them across the local community.

The initiative periodically conducts awareness workshops on fundamental concepts of information security. Addition- ally, it showcases numerous videos gathered from various international sources specializing in computer security. Furthermore, the initiative provides the option for personal assessment of information security levels through electronic tests to measure self-awareness and user qualification. The initiative also offers guidance services indirectly through short messages on mobile phones, various social media platforms such as Twitter, Instagram, or YouTube, and by providing numerous informative publications and videos.

Despite the importance of this initiative, several challenges affect its efforts, including:

A. This initiative focuses solely on educating and raising awareness among employees of official institutions, neglecting various segments of the local community. The safe use of communication technologies poses a challenge for the entire community, impacting all its facets rather than targeting specific groups.

B. The initiative relies on self-awareness, personal responsibility, and individual initiative in many non-directive guidance activities. This approach may not be suitable for our communities.

C. Additionally, the initiative lacks practical application in training, opting instead for theoretical education on fundamental information security concepts. This method of awareness may not yield favorable results, especially when directed at non-specialized, non-full-time employees.

2. Protection Initiatives

"Protection" is a group of specialized Saudi volunteers united by their commitment to national service in the field of cybersecurity. The group aims to become a reference in information security in the Kingdom of Saudi Arabia. Its main objectives include:

10.1. Disseminating the concept of information security to raise awareness and scientific knowledge

b. Building a database in Arabic, especially in the field of information security and its specialists.

10.2. Supporting the community and university students with informational resources related to information security

d. Encouraging specialists and researchers to participate in specialized research, report writing, and periodic articles contributing to the development of information security.

10.3. Providing a link between "Protection" and government entities for development and knowledge transfer

10.4. Offering educational content on information security

The "Protection" initiative comprises several specialized sub-initiatives in information security:

10.5. Initiative for Information Security Recommendations: Focused on dealing with electronic threats faced by institutions

b. National Center Initiative to Support Information Security: Aimed at supporting small and medium-sized institutions in the Kingdom.

c. Initiative to Recommend Support for Information Security Certifications: Part of a program for human resource development.

Despite the significance of these initiatives in serving the local community and enriching it with specialized research and consultations in information security, the researcher believes they need to adopt a clear plan to elevate the knowledge level of the nation's individuals. This transition is crucial for fostering a security-conscious culture, achievable through continuous training programs accessible to all segments of society.

11. Awareness Campaign

This campaign was established in the Sultanate of Oman in alignment with Oman's digital strategy for transitioning to a secure information society. The campaign targets all ministries and government institutions as part of the activities of the National Information Security Campaign, bearing the slo- gan "Towards a Safe Electronic Environment." The campaign commenced in 2009 and is considered one of the activities of the National Center for Information Security.

The campaign took the approach of training trainers and qualifying specialized teams to execute training and awareness programs related to cybersecurity. It earned the title of the Unified Campaign due to its implementation of a unified program for all employees of institutions and government departments. The aim of this campaign is to enhance awareness and raise the cultural level of individuals by familiarizing them with the best

security practices, ultimately reducing potential losses from the risks of modern electronic communication technologies.

Despite the quality of the objectives underlying this campaign, the researcher identifies some drawbacks that may diminish its intended benefits, including:

A. The initiative lacks a comprehensive understanding of community awareness, as it is limited to employees of the state and government institutions only.

B. Community protection requires an initiative that ensures a shift in the mindset of the community members regarding electronic security behaviors, rather than focusing solely on specific employees and positions.

C. This campaign does not include any programs for performance evaluation or measurement of the level of security awareness and its effectiveness among institutional individuals.

12. Information Security Program Project

This project was established in Abu Dhabi as part of the comprehensive framework for the quality management process to ensure the confidentiality, integrity, and availability of services, data, and health for the government of Abu Dhabi and its users. The project was launched by the Abu Dhabi Food Control Authority. The working team prepared a set of papers incorporating global best practices tailored to the specific needs of the government of Abu Dhabi.

The objectives of this project include enhancing the readiness of all employees in their responsibilities related to information security. This is achieved through exposing them to awareness courses and workshops specific to information security, qualifying employees to understand how to protect the information they handle. Once again, the researcher emphasizes the importance of such projects, which contribute to enhanc- ing employee readiness, awareness, and academic capacity to face impending electronic threats. However, such projects and initiatives must carry the meaning of complete societal engagement. The researcher sees the necessity of adopting an initiative or project that includes all segments of society, transforming individual culture into a culture of secure behaviors when using any of the new digital communication technologies.

13. Awareness Project for Bahraini Students

The Kingdom of Bahrain has also seen various efforts in the field of raising awareness about information security risks. The Directorate of Electronic Commerce and Information Technology at the Ministry of Industry, Commerce, and Tourism, in collaboration with the Student Activities Unit at the Ministry of Education, announced an awareness campaign for school students regarding the regulation of electronic commerce. The goal is to raise awareness levels among male and female stu- dents regarding information security risks.

It's worth mentioning that awareness campaigns have a positive impact on students. However, upon examining the details of this project and many similar projects, the researcher notes the following:

13.1. This project relies heavily on theoretical educational lectures and includes minimal practical training

b. The training in this project covers many topics related to internet applications and electronic commerce in daily life areas. However, the training duration is short, making it insufficient for adequately training students.

Top of Form

14. Awareness Campaigns

Numerous temporary and short-term awareness campaigns are frequently launched in all countries of the region, given the significant threat they pose to the security of societies in general. The following are examples of various campaigns in different Gulf Arab regions:

A. Microsoft Saudi Arabia, in collaboration with government and private institutions and civil society organizations, conducted an awareness campaign named "Internet Security and Safety." This campaign targeted school students, aiming to warn them about the risks of modern digital communication security. Led by the Saudi Communications Authority, the campaign seeks to raise awareness among all institutions and students about information security matters, aiming to minimize potential damages.

B. The Oman Electricity Transmission Company implemented an information security awareness campaign for its employees. This campaign targeted the company's employees and lasted only two days. Its goal was to enhance employees' efficiency by familiarizing them with the risks that the company's data might face due to negligence and not paying attention to some unsafe behaviors.

C. The Information Technology Department at Al-Majmaah University initiated an information security awareness campaign with the aim of raising digital security awareness, striving to achieve a safe university environment. The administration drew up the necessary plan to raise awareness among all university staff regarding information security, making them capable of recognizing the risks they might face to take caution and care.

Despite the importance of these awareness campaigns, their benefits are not sustainable and do not effectively guarantee the protection of society from internet risks. These campaigns are described as short-lived, lasting no more than a few hours per day or one day at most. These campaigns conduct workshops predominantly focused on theoretical awareness. Many employees and students have pointed out that while they know a lot about information security, they need sufficient practical experiences and continuous awareness to keep up with the evolving threat posed to them and their society.

In the next section, the researcher will present the extent of the Saudi Arabian community's interest in using the internet and the digital communication revolution, especially social media sites. Additionally, the study will explore the level of knowledge among this demographic regarding information security.

Impact of social media on the Electronic Privacy of Students in Saudi Society

This section of the study addresses key aspects to un- cover the relationship between social media and user privacy breaches, as follows:

15. **Assessing the extent of the use of various social media platforms**
16. **Understanding the objectives of students in using social media**
17. **Determining the percentage of those who have experienced security breaches and electronic extortion attempts**
18. **Identifying the level of awareness regarding the risks associated with dealing with social media**

Several questions have been raised to answer these focal points, aiming to understand the real reasons behind the vulnerability of this demographic, which forms the foundation of future societies.

This study seeks to answer these questions to derive recommendations that can mitigate security breaches resulting from inappropriate use of social media. The questions include:

19. **What is the level of enthusiasm for using various types of social media?**
20. **What are the objectives of students in using social media?**
21. **What is the level of exposure to security breaches and attempts of electronic extortion?**

4. What is the level of awareness regarding the risks associated with dealing with social media?

According to official statistics from the Ministry of Education in Saudi Arabia, the number of male and female students in both intermediate and secondary stages is 1,205,000. Based on scientific statistical measures, the required sample size for studying the research community mentioned above should not be less than 390 cases. In this study, we chose four main factors for the case study: gender, educational stage, economic level, and the number of hours used daily.

22. Results Analysis

The first axis of this study focused on understanding the extent of the enthusiasm for using various social media platforms among students. The researcher formulated nine different questions to serve this axis. Among the key results derived from the answers of the selected sample:

- **56% of students use social media for more than 3 hours and less than 6 hours daily.** Meanwhile, 44% of students use these platforms for between one and three hours daily. This high percentage indicates a significant interest among students in using these platforms.
- **62.6% of students use social media extensively,** while 32.9% use them to a moderate extent. This suggests a prevalent and substantial usage of social media among the student population.
- **79% of students use more than one account on these platforms.** This highlights a trend of maintaining multiple accounts for different purposes.
- **87.6% of students find it difficult to abstain from using these platforms.** This underscores the addictive nature and significant reliance on social media among students.

These results collectively paint a picture of the high engagement and reliance on social media platforms within the stu- dent community. The majority of students spend a consider- able amount of time on these platforms, use them extensively, maintain multiple accounts, and find it challenging to reduce or eliminate their usage. This information is crucial for understanding the impact and influence of social media on the daily lives of students in Saudi society.

Regarding the Overall Level of Interest in Using social media, the overall level of interest in using social media platforms within the study's sample was 2.2821 out of 3, indicating a very high level of interest. The average standard deviation for the first axis, as shown in the table, was only 0.37. This low standard deviation suggests minimal data dispersion, and the indicated level of interest is very close to the actual values. This high level of interest, as reflected in the overall score, underscores the significance and prevalence of social media usage among the study participants. The low standard deviation further indicates that the responses were consistent, and the average interest level is a reliable representation of the sample's sentiments towards social media usage.

As an analysis of the Second Axis - Objectives of Students in Using social media, The second axis focuses on understanding the objectives of students in using various social media platforms. This axis aimed to uncover the underlying reasons for the substantial interest in using this technology among students in the community.

- **Presentation of False Images:**
- 15.2% of students admitted to presenting false images while using these platforms.
- 23.2% stated that the information in their profiles is not genuine.
- 34.4% confirmed establishing deceptive relationships through these sites.
- **Privacy Concerns:**
- 30.4% rejected complete parental access to their accounts.
- 29.7% partially rejected parental monitoring.

These percentages highlight the prevalence of negative uses among students, potentially leading to privacy violations and ideological damage. On the positive side, many students indicated using these platforms for academic purposes (81.3%), marketing products (47.6%), and entertainment (95.5%).

This dual nature of social media use suggests both positive and negative impacts on students, emphasizing the need for a balanced approach and awareness regarding the potential consequences of online activities.

For the analysis of the Third Axis - Cybersecurity Incidents and Extortion Attempts, The third axis aims to reveal the extent to which this group is exposed to cyber-attacks and electronic extortion attempts. The results were quite noteworthy:

- **Incidents of Hacking and Theft:**
- 22.2% of students reported being hacked at least once while using social media.
- 34.7% experienced the theft of their private messages.
- 15.2% had their files and personal images stolen from their devices.
- **Extortion Incidents:**
- 15.5% claimed to be victims of continuous extortion attempts.

These findings were surprising and require urgent attention and solutions to address the potential risks and create a safer digital environment for the community.

The average for the third axis, representing the degree of exposure to hacking, was 0.48973 out of 3, indicating a relatively low level of exposure. The standard deviation was 1.4759, implying a considerable variability in the responses.

The fourth axis focuses on the cognitive level of students regarding the dangers of interacting with social media platforms without adequate security measures. The study revealed a pressing need for awareness among students on this matter:

- **Trust and Security Knowledge:**
- 58.8% accepted any friendship request on social media.
- 38.9% believed all information posted on these platforms.
- 65.6% considered social media safe and trustworthy.
- 64.6% used the same password for an extended period without changing it.
- **Security Practices:**
- More than 30% did not use any security software. 31.2%
- of those using security software did not update it.

These behaviors indicate a lack of awareness among students about the risks of unsafe internet practices. These misconceptions and practices could jeopardize the community's cybersecurity in the future if not addressed.

Proposal for a Secure Family Program:

The proposed solution focuses on preparing and training trainers to empower them to educate students about safe usage of modern communication devices. The proposal encompasses several axes:

23. E-training for Trainers:

- Provide diverse training courses for trainers associated with all stages of general education.
- Aim to equip trainers with practical skills to address electronic threats effectively.

24. E-training for Parents:

- Train trainers to educate and assist parents in raising and monitoring their children in the digital world.
- Utilize practical applications to enhance the ability of trainers to instruct parents effectively.

25. Comprehensive Security Recommendations:

- Provide guidelines and practical measures to contribute to preventing risks associated with online exposure.
- Empower trainers to educate both students and parents about the importance of online privacy and security.

Implementation Methodology:

- **Simulation-Based Learning:**
- Emphasize experiential learning by creating simulated scenarios that mimic real-world situations.
- Conduct practical exercises that allow trainers to realistically protect electronic privacy and prevent breaches.
- **Distribution of Tablets:**
- Allocate an electronic tablet to each trainer for training purposes to ensure equal opportunities for all.
- **Limit Participants per Session:**
- Restrict the number of participants in a single session to 30 to facilitate dialogue and opinion exchange.
- **Electronic Presentation:**
- Use electronic slides during lectures for effective material presentation.
- **Secure Online Platform:**
- Provide trainers with access to a secure online platform with individual passwords.
- Include all training exercises to allow trainers to review applications multiple times, reinforcing the information significantly.

The proposed solution aims to create a comprehensive program that addresses the challenges of online security, involving both trainers and parents in educating students about responsible and secure online behavior.

Expected Achievement Upon Completion of the Program:

26. Understanding of Information Security and Modern Cybercrimes:

- Acquire knowledge about information security nature and modern cybercrimes.

27. Skill in Following Proper Scientific Procedures for Password Selection:

- Develop the skill of choosing strong passwords through proper scientific procedures.

28. Encryption of Electronic Correspondence:

- Acquire the skill of encrypting electronic communications.

29. Email Preparation Skills:

- Develop the skill of preparing emails.

30. Account Recovery Skills:

• Acquire the skill of recovering electronic accounts in case of loss.

31. Remote Device Control Skills in Case of Theft:

• Develop the skill of remotely controlling the device in case of theft.

32. Secure Locking of Communication Devices:

• Acquire the skill of securely locking communication devices.

33. Safe Electronic Browsing Skills:

• Develop the skill of safe electronic browsing.

34. Prevention of Surveillance through External Control of Camera and Audio Device:

• Acquire the skill of preventing surveillance through external control of the camera and audio device.

35. Control of Social Media Settings to Prevent Any Breach:

• Develop the skill of controlling social media settings to prevent any breaches.

36. Early Detection of Breaches:

• Acquire the skill of early detection of breaches.

37. Data Privacy and Protection:

• Develop the skill of retaining and protecting data privacy from dissemination.

38. Awareness of Steps to Report Suspected Breaches:

• Understand the necessary steps to report suspected breaches.

39. Safe Reception of Emails and Secure Interaction with Electronic Friends:

• Acquire the skill of safe email reception and secure interaction with electronic friends.

This comprehensive program aims to equip participants with a wide range of skills and knowledge to navigate the digi- tal landscape securely, protecting their privacy and guarding against cyber threats.

Practical Experience:

To assess and evaluate the program practically, the researcher conducted a test with a group of students from various disciplines at a university in the Kingdom of Saudi Ara- bia. The program's first phase was implemented over two days, during which participants were trained on practical exercises. To measure the quality of the educational outcomes for students, the researcher distributed a questionnaire to assess the level of knowledge before the training program, and the same questionnaire was used after the program implementation. The responses from these questionnaires were compiled, and the quality of the learning outcomes was verified. The results of the questionnaires illustrate the difference in the level of knowledge before and after the training program.

Future Outlook:

As a result of this study, which demonstrated the significant and urgent need to equip the next generation with the skills for safe use of modern communication technologies in all their forms, such training represents a crucial step toward building a secure society. This is particularly crucial given the various forms of systematic disruption the society faces, including ethical, ideological, and intellectual challenges. In light of these findings, the researcher suggests proposing to the relevant authorities the inclusion of a security proficiency test as a requirement for university admission programs at both local and regional levels. This test should be designed similarly to the existing standardized tests for various academic subjects.

References

[1] H. Kruger, S. Flowerday, L. Drevin, T. Steyn (2011).
[2] M. Boujettif, Y. Wang, Constructivist Approach To Informa- tion Security Awareness In The Middle East, 2010 International Conference on Broadband, Wireless Computing, Communication and Applications (2010).
[3] A. A. Aldossary, A. M. Zeki.
[4] A. Oksanen, T. Keipi, Young people as victims of crime on the internet: A population-based study in Finland, Vulnerable Child. Youth Stud 8 (4) (2013) 298–309.
[5] S. Talib, N. Clarke, L. Furnell, S, M, An Analysis of Information Security Awareness within Home and Work Environments, at the International Conference on Availability, Reliability and Security (2010).
[6] M. Bidgoli, B. P. Knijnenburg, J. Grossklags, When cybercrimes strike undergraduates, in: 2016 APWG Symposium on Electronic Crime Research (eCrime), 2016, pp. 1–10.
[7] S. Markham, A, Expanding Security Awareness in Introductory Computer Science Courses. Paper presented at the InfoSecCD '09, Kennesaw, GA, USA, 2009.

[8] M. North, M. George, R. North, S, M, A Brief Study of Information Security and Ethics Awareness as an Imperative Component of Management Information Systems, Winston-Salem, N. Carolina, USA, 2007.
[9] J. Gross, B. Rosson, M. Beth, End User Concern about Security and Privacy Threats, in: Paper presented at the Symposium On Usable Privacy and Security (SOUPS), 2007.
[10] A. Alarifi, H. Tootell, P. Hyland, A Study of Information Security Awareness and Practices in Saudi Arabia, The 2nd International Conference on Communications.
[11] A. Marks, Y. Rezgui, A comparative study of informatioin security awarness in higher education based on the concept of design theorizing, Paper, Management and Service Science (2009).
[12] M. Aliyu, A. O. Nahel, N. A. Abdallah, Lasisi, Dahir diyar, ahmed m. zeki and akram m. zeki. investigating the student's awareness on computer security and ethics. computer applications: Theories and applications, IIUM Press, pp. 978–967.
[13] C. Eickhoff, P. Dekker, A. P. Vries, Supporting children's web search in school environments, in: Proceedings of the 4th Information Interaction in Context Symposium Nijmegen, ACM, 2012, pp. 129–137.
[14] O. Findahl (2009). [link].
URL http://www.lse.ac.uk/media@lse/research/EUKidsOnline
[15] I. Kabakci, H. Adabasi, A. Coklar (2008).
[16] V.J. Rideout, U. G. Foehr, D. F. Roberts, Generation M: Me- dia in the Lives of 8-to 18-Year-Olds, Henry J. Kaiser Family Foundation, Oakland, California, 2010.
[17] S. N. Hamade, Parental Awareness and Mediation of Children's Internet Use in Kuwait, in: 12th International Conference on Information Technology - New Generations, 2015, pp. 640–645.
[18] G. Mesch, Parental Mediation, Online Activities and Cyberbullying, Cyber Psychology and Behavior 12 (4) (2009) 387–393.
[19] C. Ponte, J. A. Simões, Asking parents about children's internet use: comparing findings about parental mediation in Portugal and other European countries. InEU Kids Online- Final Confer- ence, London.Available at (2009).
[20] F. Eurobarometer (2008).
[21] J. Žufić, T. Žajgar, S. Prkić, Children online safety, in: 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017, pp. 961–966.
[22] K. Strater, H. Richter.
[23] D. M. Springer (2011). [link].
URLhttp://krex.kstate.edu/dspace/bitstream/handle/2097/7299/DustinSpringer2011.pdf?sequence=1(2005).