E-Safety Awareness of Saudi Youths: A Comparative Study and Recommendations

Nawaf F Alharbi , Dr Ben Soh, Dr Mohammed A AlZain , Mawaddah F Alharbi

1st &2nd Department of Computer Science and Computer Engineering, La Trobe University, Australia
3rd College of CS & IT, Taif University, KSA, 4th Umm Alqura University, KSA

Abstract
The use of the internet has become a basic need for many across the globe. The situation is very much the same for the youth in many countries like Saudi Arabia who have grown up surrounded and accessing the internet. This demographic, however, is at an increased risk of falling as victims to cybercrime because of a low level of technical awareness. This review looks at the level of technical awareness of internet use in 3 different countries which include the USA, South Africa, and New Zealand. The review will compare the situation in these nations with those in KSA. Based on the review and comparisons, recommendations are made for culturally and socially acceptable e-Safety awareness of Saudi youths.

Keywords: *E-Safety Awareness, Comaprative Study, cyber-security threat awareness.*

Introduction

The importance of the internet in the daily lives of individuals is on the rise, more so, among the youth globally. Children are exposed to the internet at an increasingly younger age with the proliferation of internet enabled devices making it easier for them to access the internet. Overall, the internet holds the potential for positively impacting the youth. Children and teenagers can access educational content, books, and entertainment by using the internet. Communication has also massively improved with advances in technology with the young a big part of the social media and online gaming space. However, there are dangers associated with internet use among the world's youth. Issues such as internet addiction, exposure to violent and inappropriate content, and poor social skills have also been associated with increased internet usage among the youth (Hassan, Alam, Wahab and Hawlader, 2020). These challenges have necessitated the need for parents and children to be well informed on safe internet use (Vo, Locke, Johnson and Marshall, 2015). This literature review will look at studies done on awareness systems of internet use among the youth in different countries like the United States, South Africa, and New Zealand. A comparison will be made of models from those nations with the one in place in Saudi Arabia. The current Saudi model and its issues will also be discussed with additions proposed from other nations' models.

Background

A study conducted by Chen et al. indicated that a lack of security awareness was a major reason for internet insecurity in many organizations around the globe. Information security threats can come from internal or external sources. The threats also differ depending on whether it is attributable to human or non-human factors. Natural disasters are examples of external threats that people have little control over. Issues like hackers, employee misconduct, security errors, and negligence are examples of internal threats that are easier to manage through increasing awareness of information security risks (Chen, Shaw and Yang, 2013). The research conducted by Chen et al. is justified by similar concerns that inspire the inquiry into assessing the level of technical awareness among the youth in Saudi Arabia. The main threats to information security that were identified for the organization included virus infections, insider abuse, and denial of service attacks. Computer virus attacks remain the most common risk to information security globally. Viruses can come about through visiting suspicious sites as well as through spam emails. Insider abuse was quoted as the second most common threat to information security followed by denial of services attacks (Chen, Shaw and Yang, 2013). Other major threats to information include the use of Trojans, phishing, and intellectual property laws. A lack of awareness of information security and its technical aspects can render any advanced technological protection measures in place useless against these growing threats.

Manuscript received November 5, 2021
Manuscript revised November 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.11.25

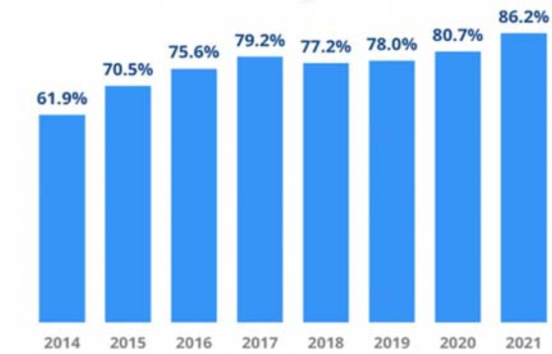

Figure 1 Percentage of organizations by at least one successful attack.

Figure 1: Percentage of organizations compromised by at least once successful cyber-attack over time.

The danger of the various threats differs in their severity as shown in figure 1. Viral attacks are the most common and can cause great harm to information systems. Computer viruses can corrupt files, distort information, and even lead to major crashes with massive loss of information. Awareness of potential sources of computer viruses in addition to effective ant-virus software can help reduce the incidence and severity of computer virus attacks. Denial of services attacks is another major threat that is facing the information security of the company. Finally, insider abuse was seen as a major threat to the safety of information security in the company. The abuse can be intentional or accidental due to a lack of knowledge on best practices for safe use of the internet and data. The issue of insider abuse remains significant especially in companies with little effort put in place to educate its workforce. These attacks lead to losses of several billions of dollars each year.

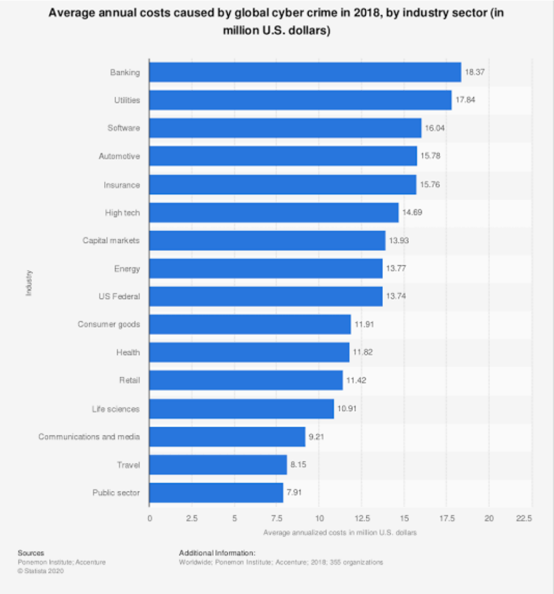

Figure 2 average annual costs by global cyber-crime in 2018 by industries

Comparative study of awareness Systems: Current awareness systems of internet usage by youth used in the USA, South Africa and New Zealand are compared with that in Saudi Arabia, as follows.

Manuscript received November 5, 2021
Manuscript revised November 20, 2021
https://doi.org/**10.22937/IJCSNS.2021.21.11.25**

USA vs. Saudi Arabia

The United States is home to the largest portion of internet consumers in the globe. The nation is a leader in technology use in many aspects of its social and economic structure. Young children in the nation are some of the biggest consumers of electronic technology, online gaming, and social media. The high internet penetrance in the country has raised concerns over the safety of children and the impact that internet use has on their health and wellbeing (Błachnio et al. 2018). Concerns over the safety of young users from cyberattacks are also increasing with cases of fraud, identity theft, phishing, and hacking ever present online. According to the FBI, 500,000 to 700,000 new Americans fall victim to identity theft each year with young users the most vulnerable victims. Bruijn and Janssen (2017) noted that although cybersecurity was a global phenomenon that presented complex socio-technical issues to governments, there was little done in terms of increasing awareness of the threat. In the United States, cybersecurity awareness programs that target young users are numerous with no clear national standard set. Different states have their individual cyber security awareness programs and initiatives targeting different groups in society mainly young children and teens. Private organizations also play a role in increasing awareness of online threats to users through educational programs and collaborations with learning institutions.

The United States government also plays an active role in increasing awareness on cyber-security among the youth. The establishment of the Cybersecurity and Infrastructure Security Agency (CISA) is considered one of the most significant ways that the federal government can tackle online threats to its systems and its citizens. CISA mainly deals with investigating and defending against cyber-attacks from malicious players and nations. According to Asokan (2021), the Biden administration is seeking to increase the budget allocation to CISA by $110 million to boost efforts of increasing the public's awareness of cyber threats that exists when one uses the internet.

The interplay of state and national government efforts for increasing awareness of internet usage among the youth in USA along with private players makes its programs more widespread than in Saudi Arabia. Aljabri (2021), conducted a study assessing the levels of cyber security awareness in Saudi Arabia and how cyber-crime could be tackled. The author noted that like the United States, the Saudi government had put in place laws seeking to protect citizens from online crimes. However, the nation did not have a centralized body like America's CISA to coordinate internet use awareness programs across the nation. Other major differences noted by the author between Saudi and USA that the cyber-crime laws in Saudi Arabia were guided more by cultural and religious inclination compared to those seen in the USA. The USA has a much more complex and better developed cyber laws because of higher access to the internet. The jail terms also differ with the US laws having stricter penalties for unauthorized access to someone's data. Cyber security awareness programs in Saudi are also fewer and less well-defined.

Awareness of internet use and cyber security threats among the youth in South Africa remains low compared to Saudi Arabia. Venter et al. (2019) looked at awareness levels among South African youth on basic cyber security terms and threats. The authors noted that the nation had experienced a significant rise in internet use over the past three decades. Much like Khan and Gadhoum's (2018) study, Venter et al. (2019) attributed the increase in internet access in South Africa to a proliferation of availability and affordability of smart phones. The young in South Africa, however, had little awareness on how to keep their devices secure from external threats. A major reason for the low internet use awareness levels in the country is because the knowledge is often preserved for those pursuing computer related courses in higher education facilities. The authors noted that the nation requires a robust internet use awareness program that would be available at all stages of education including primary and secondary school students. Comparatively, Saudi Arabia's internet use awareness program remains limited although it has a better penetrance among younger children in schools.

1. *New Zealand vs. Saudi Arabia*

2. *South Africa vs. Saudi Arabia*

The growing research into internet use and surveillance among the young in New Zealand is indicative of the overall growth of internet use worldwide. According to Tirmula and Sarrafzadeh (2016), a majority of students in New Zealand were not aware of cyber security threats and the dangers associated with the use of the internet. The study was conducted because of the increase in internet usage among students in the country. Much like in Saudi Arabia, many of the young school going children in New Zealand have access to the internet either through a home computer, a smart phone, or a tablet. The youth are accessing content online at an increasingly younger age with concerns over the impact it will have on their overall safety. Access to the internet means that there is a higher vulnerability to cyberattacks. The authors of the study looked at how internet use and the introduction of e-learning as well Bring Your Own Devices programs in most schools made the use of internet a common thing for teachers and students. However, a small portion of teachers and students who took part in the study were aware of cyber security threats that are common. The online survey conducted on children aged between 8 to 12 years had a completion rate of just 19% with the children having little awareness of the existence of cyber security threats need for urgent cyber security awareness programs among students in the country.

The situation in New Zealand is almost like that of Saudi Arabia that lacks a formal internet usage and cyber security awareness program in place. The two countries both have a young generation that is increasingly becoming dependent on technology for activities such as learning, communication, and entertainment. Both Saudi Arabia and New Zealand have a high internet penetration rate with no clear state like phishing or hacking. The paper emphasizes the run cybersecurity awareness program in place. A validation system is needed in both countries which targets the young children and improves their knowledge of cyber security and its application to their use. According to Khan and Gadhoum (2018), the cases of internet addiction is on the rise amongst the youth in Saudi Arabia with a growing need to increase awareness of the dangers associated with increased internet use. Table 1, gives summary of differences in relation to e-Safety initiatives in the four nations.

Category/Country	Saudi Arabia	United States	New Zealand	South Africa
Level of Awareness on Cybersecurity among the Youth	The awareness levels shows gaps that exists in cyber security knowledge especially among the very young citizens	Level of awareness cannot be accurately measured since cybersecurity awareness programs that target young users are numerous with no clear national standard set.	A majority of students in New Zealand were not aware of cyber security threats and the dangers associated with the use of the internet	The youth's awareness of cybersecurity threats are low but is on a fast rise with increased internet penetrance.
Role of Government	The Saudi authorities set up an e-learning program in the early 1990s that to increase technical knowledge on internet use. The National Communication and Information and Technology plan was enacted in 2007 to promote ICT education in schools	Different states have their individual cybersecurity awareness programs. The role of government is therefore scattered across states.	New Zealand's government plays a minimal role in raising awareness of cybersecurity threats among the youth.	Currently government has a minimal role in raising awareness of cyber threats among the youth.
National programs present	National Communication and Information and Technology plan in 2007	The US has set up CISA to tackle online threats at the federal level.	None	None
Internet Use amongst the Youth	Very High	Very High	Very High	High

Table 1: Main differences in internet and cyber-security threat awareness among youth in the four nations

2. *Current Saudi Arabia e-saftey and issues*

The impact of the internet on the youth in Saudi Arabia has been significant. Saudi Arabia, like many other countries in the Gulf region, is young and urban. A majority of the young in KSA are concentrated around cities like Riyadh, Mecca, Jeddah, and Medina. Approximately slightly more than half of the estimated 33.5 million population in the kingdom is below the age of 30. When Saudi nationals are considered independently, the percentage of under 30 rises to more than 60% with 40% being below the age of 18 (Alaoui, 2019). The large young demographic in KSA are heavy consumers of the internet. Internet penetrance is high among KSA due to increased connectivity, easier access to internet-enabled mobile devices, and the rise of popular social media platforms that attract the youth. The demographic structure seen in KSA resembles that observed in South Africa where the majority is composed of the youth. Internet use amongst the young in KSA affects how the youth communicate, interact, learn, earn, and even voice political opinions. The increased use of the internet among the young in KSA also exposes the country to online threats since the demographic is at an increased risk as a target for malicious players. There is an outstanding need for raising awareness among the youth in KSA on the technical aspect of internet use to improve overall safety when using the internet.

In Saudi Arabia, the current level of awareness shows gaps that exists in cyber security knowledge especially among the very young citizens who are at an increased risk of falling victim to online dangers. The authorities in Saudi Arabia have made concerted efforts over several years to increase the level of knowledge on internet use among its population. The Saudi authorities set up an e-learning program in the early 1990s that sought to increase the technical nature of National Communication and Information and Technology plan in 2007 internet and technologies. The e-learning program was further supported by the authorities by setting up the to ensure that ICT education was present at all learning institutions in the country. The program saw the integration of ICT education in the curriculum of schools across the country where children were taught on basic facts and knowledge on the use of ICT and the internet to promote cyber-security and awareness of the dangers that may exist online. The e-learning program, however, has recently gone through changes that has seen the e-learning program confined to higher education institutions that has led to a big gap in adequate knowledge for the younger children in lower classes. Much like in South Africa, the situation in Saudi Arabia leaves the young children particularly vulnerable to an array of cyber threats as they access the internet more frequently. The gap in knowledge in this age group has raised the need for an effective system that will help increase the technical awareness of internet use in KSA so that they can avoid dangers and mitigate threats.

The authorities in KSA have more recently signed a memorandum with DQ to utilize a framework for raising digital awareness among children in the country. The newly adopted DQ framework is a novel world class and accepted standard approach for increasing digital literacy as well as improving the safe use of the internet among the youth. The memorandum was signed with the goal of contributing to the increasing positivity of technical outputs for the future generations. The framework aligns with the agenda of the C20 Civil Society Communication Group Forum (Salama, 2020). The framework is meant to measure its effectiveness using the Child Online Safety Index (COSI). The index assesses online safety amongst minors by looking at 6 main pillars. These pillars include disciplined digital use, social infrastructure, cyber risk, competency, digital connectivity as well as education (Balhara, Harshwardhan, Kumar and Singh, 2018). Saudi Arabia plans to utilize the framework and the COSI to improve online safety for the youth in the kingdom. The program, however, is in its early stages and requires more monitoring to determine its effectiveness among school-going children.

A look at the growth pattern of internet use in Saudi Arabia shows that the younger children are spending more time online than ever before. The high internet penetration rate in Saudi Arabia coupled with the growing demand for smart phones means that more children are accessing content online more than ever before. At least 70% of children aged between 8 to 18 years old in the Gulf countries own a device that can access the internet including smartphones, tablets, and personal computers (Livingstone, 2019). The situation is similar for even younger children with an estimated 23% of 5 to 9 year olds having access to the internet. Online gaming and social media platforms are the most popular amongst young children with many spending most of their free times engaged in these activities. This young demographic in Saudi Arabia spend an inordinate amount of time online but with very little awareness of the technical aspects of internet use and the possible threats that exists. Young children online, therefore, are more likely to fall victim to identity theft, phishing attacks, and credit card fraud as they access the internet (Mark and Nguyen, 2017). A comprehensive system is required to increase the information made available to young children and their guardians on the safe use of the internet.

3. *Recommendations*

After closely analyzing the different levels of technical awareness on internet usage among the young in different countries, we observe there are some few exceptional practices that Saudi Arabia can adopt in its internet awareness program. One such idea is involving the private sector beside the public sectors in increasing outreach to more young Saudis much like in the United States where the private sector plays a role in increasing awareness of internet use and the dangers associated with the same. The public sector is constrained by financial and bureaucratic bottle-necks making service delivery slow and at time inefficient. The private sector with the public sector can play an active role in reaching out to more people with information on the safe use of the internet especially among younger children. The Saudi authorities should offer incentives to private companies beside the government programs to carry out educational programs in lower grade classes.

The concept of private firms playing an active role in improving digital awareness is not new to KSA. KSA authorities had set up the “Kulluna Online” program in 2017 that promoted the safe use of the internet and digital literacy amongst school-going children. The program was a collaborative effort involving the Prince Mohammed bin Salman Foundation and Google. The program was a niche concept that sought to include students from across the country in interactive workshops led by Google facilitators. The program initially started with 10,000 students from 50 schools in Riyadh to take part with plans of expanding to many other schools across the entire kingdom (Shalhoub, 2021). However, unlike the efforts seen in the US, Kulluna Online was limited to one private player Google making its rollout slower and more costly to the partnering organizations. The authorities in KSA recognize the importance of involving non-governmental organizations, private and non-profit companies. Involving private firms will increase the outreach of digital awareness and safety among the youth (Kavallieratos, Katsikas and Gkioulos, 2020). The move also reduces the associated cost of increasing awareness since it is shared between the government and the company.

Borrowing from the United States model, Saudi Arabia should consider creating a central organization that would be in charge of creating awareness on internet usage much like America’s CISA. The body should be in charge of coordinating the education program and monitor the various dangers that are associated with increased and uncontrolled internet usage among the youth. A centralized body with the mandate of increasing technical use of the internet amongst Saudi Arabian will have several advantages. The first is the adoption of a kingdom-wide standard approach to increasing technical awareness of internet use. A centralized body, rather than regional ones, can give better direction and execute more effective actions with the goal of increasing awareness (Sharma and Manocha, 2020). The second benefit of a centralized authority is the availability of funding and political support. A central body elevates the importance of raising awareness at the national front and makes it easier for programs to receive financing and support.

From the New Zealand model, Saudi Arabia can incorporate the involvement of teachers in its program. Much like Saudi Arabia, New Zealand lacks a formal national internet awareness program for its young population. Teachers in schools, therefore, are usually the main source of information on internet use for children. The role of the teacher in disseminating information to a large population of students cannot be underestimated. In Saudi Arabia, school going children can receive basic internet usage knowledge and safety information from their teachers. Involving teachers and learning institutions will help increase awareness to a large pool of young children faster. Parents and guardians can also be included in the internet awareness program because of their proximity to and influence on the youth and their use of the internet. Parents can inform the youth on safe use of the internet, dangers that exist online, and how to avoid falling as a victim to cyber-crime.

There are no cultural or societal limitations in Saudi Arabia that would hinder the incorporation of any other ideas from either USA, New Zealand, or South Africa into Saudi’s internet awareness program. There are few internet awareness programs globally with even fewer focusing on younger children and teenagers. E-learning is mainly limited to higher education institutions leaving a large demographic of younger children vulnerable to online dangers and threats. Saudi Arabia is in a position to incorporate any new ideas that would make it easy to reach out and educate this demographic.

Cultural barriers, however, are expected to affect the effective implementation of some of the proposed additions. Issues might arise when it comes to incorporate New Zealand’s approach to internet use awareness that emphasizes on teacher and guardian participation. The youth face a host of challenges and dangers online that only increase with continued access. Online abuse, cyber-bullying, and other related online dangers to the young require that the young communicate to authority figures for intervention (Livingstone, 2019). In Saudi Arabia, open and safe dialogue about online abuse can be difficult due to the greater distance of power that exists in Saudi culture compared to that seen in New Zealand. A student in Saudi Arabia might be less likely to confide details of their internet use to an authority figure compared to a New Zealand student due to fear of reproach.

Interventions that require better communication between parents and children can also be negatively affected by the prevailing traditions, practices, culture, and norms. Parents in Saudi Arabia, for example, may be tempted to spy on the online activity of their children rather than engaging them in dialogue (Livingstone, 2019). Spying reduces trust between parents and children making it more difficult to increase technical awareness on the use of the internet and online safety.

4. *Conclusion*

Internet usage is on the rise in Saudi Arabia, especially among the young children as internet penetration increases and more people have access to internet-enabled devices. Internet usage among the youth has several benefits such as being an educational tool, improving communication, and even as a source of entertainment as evidenced by the growing numbers of online gamers in KSA. However, there is very little technical awareness among this population on the technical aspects of internet usage and cyber security. The youth, therefore, are more vulnerable to malicious attacks online compared to the rest of the population. This review looked at the level of technical awareness of internet use in countries such as the United States, New Zealand, and South Africa to compare with the current situation in Saudi Arabia. The United States does not have a formal nationwide internet awareness standard but rather relies on the different states to raise awareness locally. The private sector also plays an active role in educating the masses on the technical aspect of internet use as well as warning against online threats. The CISA also plays an active role in raising awareness of threats to the country's cyberspace. Saudi Arabia can incorporate the use of the private sector and centralized body to increase the efficiency of its awareness program as well. South Africa, much like in Saudi Arabia, has its internet awareness programs limited to higher education forums making it inaccessible to younger citizens. Finally, New Zealand also has a low technical awareness of internet use among its young population. Initiating education programs led by teachers is one way that the country seeks to address the issue. The prevailing culture and practices in Saudi Arabia do not hinder the incorporation of the proposed additions. However, existing social norms might affect the effectiveness in which it is implemented. The Saudi culture is defined by a wider power distance between the young and people of authority making open and free conversations between children and teachers or guardians more difficult. This cultural practice may negatively affect the implementation of New Zealand's approach of using teachers in raising online safety awareness. Overall, it is vital that the young generation in Saudi Arabia gain technical awareness of internet use to protect them from falling victims to online malicious actors and attacks.

References

References

[1] Aljabri, S.2021, 'Cybersecurity Awareness In Saudi Arabia.' *International Journal of Research Publication and Reviews*, Vol. 2, No. 2, Available from: < www.ijrpr.com ISSN 2582-7421>

[2] Alaoui, H., 2019. Youth, Technology, and Political Change in Saudi Arabia. *Hoover Institution*, [online] 2(519). Available at: <https://www.hoover.org/research/youth-technology-and-political-change-saudi-arabia> [Accessed 30 May 2021].

[3] Asokan, A 2021, '*Biden seeks to boost CISA's budget by $110 million.*' Bank information security news, training, education - BankInfoSecurity. Available from: <https://www.bankinfosecurity.com/biden-seeks-to-boost-cisas-budget-by-110-million-a-16377> [1 May 2021]

[4] Balhara, Y., Harshwardhan, M., Kumar, R. and Singh, S., 2018. Extent and pattern of problematic internet use among school students from Delhi: Findings from the cyber awareness programme. *Asian Journal of Psychiatry*, 34, pp.38-42.

[5] Błachnio, A, Przepiorka, A, Benvenuti, M, Mazzoni, E. & Seidman, G 2018, ;Relations Between Facebook Intrusion, Internet Addiction, Life Satisfaction, and Self-Esteem: a Study in Italy and the USA.; *International Journal of Mental Health and Addiction*, vol.17, no.4, pp.793-805.

[7] Chen, C., Shaw, R. and Yang, S., 2013. Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning, and Performance Journal*, 24(1), pp.193-205.

[8] De Bruijn, H, & Janssen, M 2017, 'Building cybersecurity awareness: The need for evidence-based framing strategies.' *Government Information Quarterly*, Vol. 34, No. 1, Available from< https://doi.org/10.1016/j.giq.2017.02.007>

[9] Hassan, T, Alam, M, Wahab, A & Hawlader, M 2020, 'Prevalence and associated factors of internet addiction among young adults in Bangladesh.' *Journal of the Egyptian Public Health Association*, vol.95, no.1.

[10] Kavallieratos, G., Katsikas, S. and Gkioulos, V., 2020. Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. *Future Internet*, 12(4), p.65.

[11] Khan, H. U., & Gadhoum, Y. 2018, 'Measuring internet addiction in arab based knowledge societies: a case study of Saudi Arabia.' *Journal of Theoretical and Applied Information Technologys*, vol. 96, no. 6.

[12] Livingstone, S., 2019. *Overcoming cultural taboos: protecting children online in Saudi Arabia*. [online] Parenting for a Digital Future. Available at: <https://blogs.lse.ac.uk/parenting4digitalfuture/2019/06/12/overcoming-cultural-taboos-protecting-children-online-in-saudi-arabia/> [Accessed 30 May 2021].

[13] Mark, L & Nguyen, T 2017, 'An Invitation to Internet Safety and Ethics: School and family collaboration. *Journal of Invitational Theory and Practice*, vol.44, no.3, pp.183-185.

[14] Salama, S., 2021. *Saudi Arabia to raise digital awareness level, boost child safety online*. [online] Gulfnews.com. Available at: <https://gulfnews.com/world/gulf/saudi/saudi-arabia-to-raise-digital-awareness-level-boost-child-safety-online-1.74486423> [Accessed 30 May 2021].

[15] Shalhoub, L., 2021. *MiSK, Google form joint initiative on children's Internet safety*. [online] Arab News. Available at: <https://www.arabnews.com/node/1054496/saudi-arabia> [Accessed 30 May 2021].

[16] Sharma, V. and Manocha, T., 2020. Cyber-crimes- Trends and Awareness: A study on Youth. *BULMIM Journal of Management and Research*, 5(2), p.63.

[17] Tirumala, SS., Sarrafzadeh, A, & Pang, P 2016, 'A survey on internet usage and cybersecurity awareness in students.' *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Vol. 2, No. 1, Available from: < https://doi.org/10.1109/pst.2016.7906931>

[18] Vo, D., Locke, J., Johnson, A. and Marshall, S., 2015. 50. The Effectiveness of the Mindful Awareness and Resilience Skills for Adolescents (MARS-A) Intervention on Adolescent Mental Health: A Pilot Clinical Trial. *Journal of Adolescent Health*, 56(2), p.S27.

[19] Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. 2019, 'Cyber security education is as essential as "the three R's".' *Heliyon*, Vol. 5, No. 12 e02855. Available from. <https://doi.org/10.1016/j.heliyon.2019.e02855>