REVIEW OF RISKS AND PRECAUTIONS IN ONLINE LEARNING: A CAUTIONARY VIEW FOR ADOPTING E-LEARNING IN DEVELOPING COUNTRIES IN THE NEW NORMAL

Lead Author:

Israel Oghenevwe de Regha

Affiliation:

Computer ScienceDepartment
Federal College of Education, Kontagora
Niger State

Abstract

The global lockdown occasioned by the outbreak of the Covid-19 pandemic led to the closure of schools in most nations of the world. This also led to global increase in the demand for online (e-learning) learning at all levels of education, including developing countries. While there are several identified benefits of online learning, there are also potential risks associated with its usage. More at risk of online learning are children and young people (Minors). Caution is therefore required to be taken while introducing this category of students to online learning amidst greater emphasis and demand for online learning in the new normal dispensation. The purpose of this study is to create awareness on the potential risks associated with studying online, especially for young students in developing countries; and also to identify the various precautions that could be employed to minimise these risks. The study was carried out using the Narrative Review methodology. Relevant literatures that focused on potential online risks and the necessary safety measures and precautions required for students to safely study online were reviewed. Based on the findings, the study recommends among others, that asynchronous learning should be more emphasizes than synchronous learning for children and young people using the internet for e-learning purpose. This and other similar measures will enhance the safety of our students while studying online especially as the demand for online education is on the increase.

Keywords: Covid-19, cyber-bullying, cybercrimes, cyber-attacks, minors, e-learning, online risks, online attacks, precautions.

Co-Authors

Onanaye, Adeniyi Samson Mathematics and Statistics Department, Redeemer's University, Ede, Osun State Nigeria. **Israel-Regha, Mercy Ninma** Business Education Department
Federal College of Education, Kontagora Niger State

Introduction

The global lockdown occasioned by the outbreak of the Covid-19 pandemic between 2020 and 2021 led to the closure of schools in most nations of the world (Zakuan & Saian, 2022; Siyam & Hussain, 2021). This also led to global increase in the demand for online learning (e-learning)at all levels of education, with many nations, institutions, parents and individuals switching to online education (e-learning) as an alternative to sustain educational activities while the lockdown last (Adelekun, 2020; Edwards, 2021; Siyam & Hussain, 2021; Mitra, 2020).

While there are several identified benefits of e-learning, there are also potential risks for users of the internet (Siyam & Hussain, 2021; Mitra, 2020; Alqahtani, 2016; Moreno et al., 2013; Chen, & He, 2013).The increase in online learning due to the covid-19 pandemic also increased the incidences of cybercrimes (Zakuan & Saian, 2022; Mitra, 2020; Ahmad, 2020). According to Mitra (2020), the incidences of "online child abuse and attempts to access them in countries such as the US, United Kingdom, Spain, Australia, Denmark, and the Philippines, have reportedly doubled or tripled since the coronavirus pandemic and resultant global lockdown".

In developed countries, e-learning is more entrenched with high digital literacy even among adolescents and with access to variety of websites for online safety lessons and advices Alqahtani (2016). Comparing digital literacy skills between students from the Gulf States with their counterparts from United Kingdom (U.K), Alqahtani (2016) observe that students from U.K are digitally more skilfully and have access to several online safety lessons than their counterparts from the Gulf States. He argues that this may help them to stay safer while using the Internet. Mascheroni and Ólafsson (2014) also observed that older users of the Internet are more skilful and resilient in overcoming attacks than new users. It can therefore be inferred that students from developing countries like Nigeria with lower digital skills and inadequate ICT infrastructure may even be more prone to cybercrimes. Sharing a similar view, Mitra (2020) posits that children from low income homes and from less educated communities are among the most vulnerable to cyber-attacks. Those who are vulnerable offline because of psychological problems or social characteristics find online risks more harmful (Livingstone et al., 2012) as cited in Mascheroni and Ólafsson (2014).

Since the outbreak of the Covid-19 pandemic and its resultant impact on education, several studies have been carried out on the subject of e-learning from different perspectives, but studies on the threats and safety of online users in developing countries are scarce. This study was carried out, mainly, to create this awareness by bringing to the fore some of the potential dangers associated with the use of the internet for educational purposes especially for children and young people. The study also suggests some safety and precautionary measures identified from reviewed literatures that are useful in minimizing online dangers.

Shillair et al. (2015) as cited in Mark and Nguyen (2017) posits that while Internet safety messages and warnings have become prevalent in the media, and serve as reminders of the online dangers that exist, not as much attention has been paid to the actual steps people should take to protect themselves and others in from such dangers. Chen andHe (2013) observe that e-learning developers give more attention to the course content than to security concerns of using it, and on the other hand users are eager to use the new technology without paying attention to security issues that might arise from it.

Consequently, it is important that government, parents, teachers and other stakeholders should critically consider online safety measures among other requirements before adopting or commencing e-learning for young people in this clime. This will help minimize online risks and maximize the benefits of online usage.

Methodology

This study was carried out using the narrative review research methodology. The reviews of literatures were done by searching for relevant scholarly articles, including journals, abstracts and published reports. Google Scholar and Google search engines were used to search for relevant articles for this study. Some of terms used to search for articles for this study include: Scholarly articles on online threats for kids and young people, scholarly articles on cyber-attacks threats on children and young people, e-learning and online risks, scholarly articles on cyber-bulling, impact of cyber-attacks on children and young people, Covid-19 and cyber-attacks on online learners, online safety measures for children and young people using the Internet, precautionary safety measures from cyber-attacks, and among others. Finally, a total of 105 articles were accessed from the search results with 25 of them analysed.

Terminologies used in the Study

Several words or terminologies are often used interchangeably (synonyms) in computing technologies. Some terms used interchangeably as synonyms in this study are hereby presented. The first synonym are online risks, cyber risks, online threats and cyber threats; the second categories are online crimes and cybercrimes; the third categories are online attacks and cyber-attacks; the fourth categories are online-safety and cyber-safety; and lastly, the term Minors, is used to connote children and young people/adolescents.

Literature Review

Online risks have been explained by many researchers as a range of online activities that could cause harm to users of the Internet (livingstone, 2013; Machimbarrena et al., 2018; Alqahtani, 2016). While all users of the Internet are potential targets of attacks, the focus of this study is on Minors.

Globally, researches have shown that there is steady increase in the use of the internet for people across all age brackets for different purposes Mitra (2020). According the scholar, the Internet now has people of ages between 2 to 65 years old as active users. Edwards (2021) also observe that children as young as 5 years old are now users of the internet either with or without supervisors. The increase in digital technological advancement in both hardware and software is one of the reasons responsible for this (Mitra, 2020).

This trend is worrisome due to increasing incidences of cyber-attacks on children and young people all over the world. Moreno et al. (2013) report that, up to a third of youth in the United States (U.S) have suffered from one form of cyber-bullying or the other with some leading to various degrees of health challenges. Similarly, the National Centre for Missing and Exploited Children (NCMEC) in the United States reported a global rise in online child abuse cases from 2 million in March 2020 to about 4.2 million by April 2020 (Mitra, 2020). This according to the author was due to increase in online presence during covid-19 pandemic lockdown.

Cybercrimes covers a broad range of issues. Some of the most prevalent cybercrimes targeted towards children and young people as seen from most of the literatures reviewed include cyber-bulling, sexting, sexual exploitations, pornography, identity theft, phishing, privacy violations, fraud, stalking, cyber grooming, unwanted solicitation, gambling, netiquette, and among others (Mitra, 2020; Machimbarrena et al., 2018; Alqahtani, 2016; Moreno et al., 2013). On the frequency of occurrence among the identified cybercrimes, cyber-bullying is reported to rank highest among cybercrimes from a global survey (Mitra, 2020;Siyam&Hussain;2021, Machimbarrena et al., 2018).

Cyber-attacks on children and young people are not always from adults. Alqahtani (2016) report that while it is commonly believed that cyber-attacks on young people are predominantly adults, incidences of cyber-bullying have also be to traced to include people of the same groups. Similarly, it is also important to emphasize that apart from cybercrimes targeted on users by some malicious persons, some online crimes are caused by users themselves, either through improper online behaviour (netiquette) or by deliberately indulging in activities such as gambling, gaming, pornography and the likes which often leads to addictions. In a study suggesting how users contribute to online attacks through improper behaviour, Moreno et al. (2013) reveals that"one-third of American adolescents had given their internet password to friends and one-fourth were unaware that content uploaded online cannot be permanently delete".

Researches have also shown that violent and other forms of improper online behaviours such as cyber bullying by young people could be "associated with poor family dynamics, as well as either too much or too little parental restrictions on technology use" (Chng, Li, Liau, &Khoo, 2015; Sasson & Mesch, 2014) as cited in Mark and Nguyen (2017).

Cybercrimes pose serious danger to children and young people with some incidence resulting into irreversible damage to victims (Mitra, 2020).For instance cyber-bullying can result into; anxiety, low self-esteem, emotional distress, depression, mental health, suicide (Bullycide),frustration, rage, grief, among others (Zakuan & Saian, 2022; Siyam & Hussain, 2021; Mitra, 2020; Mark,& Nguyen, 2017; Moreno et al., 2013). Other harmful effects of cybercrimes include sexual exploitations, kidnappings, initiations into cultism and drugs, addictions, gambling and many more. In other words, the negative impacts of cybercrimes are much. The severity of these impacts may vary from one individual to another (Zakuan & Saian, 2022)

The most vulnerable groups of children and young people prone to cyber-attacks include, children of ages 2-10 years, girls, children of low income background, out of school children, children with disabilities, children with mental health condition, children from less educated communities, children under foster care, children from broken or abusive homes, children in correctional homes (Mitra, 2020) and children with learning disabilities (Alqahtani, 2016). Mascheroni andÓlafsson (2014) posit that "children from lower income families

(13%) are twice as likely to go to an offline meeting with an online contact than children from wealthier homes (6%)".

With increasing technological advancement and more online engagement by young people, it is obvious that cybercrimes and its consequences will keep increasing to the detriment of all. Therefore, more efforts are required by all stakeholders in combating this menace.

Causes and Sources of Cyber-attacks

Researchers have identified two (2) major sources of online threats. The first is due to users and the other due to management or software providers (Chen &He, 2013). From the user's angle, some researchers pointed out that online insecurity is mainly due to lack of inadequate knowledge of users' on online safety issues and improper online behaviours (Mitra, 2020;Chen &He, 2013).

Cybercriminals like other criminals are often very subtle in nature; and most often than not capitalises on the weakness and ignorance of their victims to attack them. Below are some avenues through which children and young people can expose themselves to online attacks:

- **Access to personal details:** Alqahtani (2016) posits that one avenues predators uses to attack minors online is through their personal details (names, photos, home and school addresses, and the likes) which many of them often provides or displays on their webpages and other online platforms. Moreno et al. (2013) reported that many young people compromise their online safety by giving out their internet passwords to their friends.

- **Accepting online friendship:** Accepting online friendship with people they have never met before in real life is another identified potential source of danger for young people using the internet (Alqahtani, 2016). Lenhart et al. (2015) cited in Alqahtani (2016) reported that about 57% of American young people had made online friends with people they never knew in real life before. They went further to say that about 20% have established physical contacts with such online friends. Newsbeat (2014) in Alqahtani (2016) also revealed that about a third of the United Kingdom (UK) youths have also physically met people they only got to know online. Establishing Physical contacts with virtual friends have resulted into ugly incidences such rape, assault and even death. An example was the murder of a Nigerian lady Cynthia Osokogu in 2012 by a Facebook friend in Lagos (**Ezeamalu**,2012).

- **Viruses:** Downloading anonymous files from and accessing unknown or untrusted sites could also expose online users to viruses, hacking and other forms of attacks (Alqahtani, 2016).

- **Lack of adequate digital skills:** Another cause of online vulnerability may be due to ignorance and low technical or digital skills. Mitra (2020) posits that "low technical skills such as knowledge about privacy settings, filtering mechanisms, how to monitor security or recognise fake news – among children, young people, parents, and educators can increase the vulnerability of exposure to different kinds of risk".

On the other hand, cyber threats from the standpoint of the management centre on inadequate security features of e-learning software. Researchers argue that most e-learning providers are rather more concerned about the content of the software than the security of its users (Chen &He, 2013).

Online Protection Measures

Many studies proffering strategies and measures for protecting minors using of the Internet have been conducted (Mitra, 2020; Chen &He, 2013). Chen and He, (2013) posits that the responsibility of online safety for children and young people lies on the users and the managers. It suffices to state here that different researchers have looked at online safety from different perspectives. Consequently, online safety approaches have also been presented from different angles. However, this study limits cyber safety consideration to children and young people using the internet basically for educational purpose. Some of the measures identified and discussed below include; digital/cyber security policies, digital education, national and international collaborations, technical measures, among others.

- **Cyber security policy**: Cyber security policy is one of the identified measures of ensuring online safety for users (Mishra et al., 2022; Zakuan & Saian, 2022; Siyam & Hussain, 2021; Mitra, 2020). Mishra et al. (2022) posit that cyber security policies "refer to tools, regulations, rules, procedures, ideas, management techniques, and best practices". These documents set rules and standards that regulate the implementation and ethical use of internet in schools with the sole aim of ensuring safety for users (Siyam&Hussain, 2021). While individual schools should have an operational cyber safety policies as in the case of some developed countries like the United states of America and the United Kingdom where it is mandatory by law (Chalmers et al.2016), a broad cyber security policies should be drawn by authorized government agencies of each country (Siyam & Hussain, 2021). Therefore having a well-defined digital security policies and procedures is as important as having technical solutions (Mishra et al., 2022)

- **Online safety education:** Online safety education is another identified measure that can enhance online protection for children and young people using the internet (Mitra, 2020;Alqahtani, 2016;Farrukh, Sadwick, & Villasenor, 2014; Chen &He, 2013; Moreno et al., 2013). Ignorance and improper online behaviour increases the vulnerability of minors using the internet. For instance, Moreno et al. (2013) in their study reveal that "one-third of adolescents in the United States of America had given their internet password to friends and one-fourth were unaware that content uploaded online cannot be permanently deleted. Online safety education may help to prevent or reduce the negative impacts of cybercrimes (Moreno et al., 2013)

  Online safety education for children and teenagers should equip them with the knowledge of how to identify potential online risks and also to inculcate appropriate online behaviours (Farrukh, Sadwick, &Villasenor, 2014). In addition to detecting threats, students should also be able to know how to respond to each type of threat appropriately; for instance young people should be acquainted with "utilizing IP addresses to track and block problematic visitors, switching online user accounts if harassment begins" (Farrukh, Sadwick, &Villasenor, 2014) and other similar safety techniques. Some advocates of online safety education believe that online education should begin at a young age. In a survey study among stakeholders conducted by Moreno et al.(2013), the average age as revealed by the survey appropriate for commencing internet safety education was 7.2 years.

- **Parental safety Measures:** Researches have shown that Parents have major roles to play in the safety of their children (Mitra, 2020; Alqahtani, 2016;Chen &He, 2013; Moreno et al., 2013). Mascheroni and Ólafsson (2014) report that children spend more time on the internet at home than in school. This makes it even more pertinent for parents to be involved in protecting their children against online attacks. There are a number of ways parents can provide online security; ranging from physical restrictions and supervisions to software restrictions and monitoring (Farrukh, Sadwick, &Villasenor,

2014) and through education (Moreno, 2013). Unfortunately parents are said to be behind their children in digital expertise (Mitra, 2020;Alqahtani, 2016). It is therefore imperative for parents to also acquire sufficient digital skills to be able to provide the needed safety assistance and education to their children.

- **Collaborative safety measures:** Cybercrime like any other crime can best be fought through collaboration between all the stake holders. Mitra (2020) posit that online safety through collaborative efforts is novel and most effective approach for protecting minors against cyber-attacks. Many researchers on the subject of online safety for minors are united that Internet safety should not be the responsibility of schools alone but requires a comprehensive partnership between schools, parents, users, communities and government (Mitra, 2020; Mark& Nguyen, 2017; Alqahtani, 2016). Collaboration could foster trainings, knowledge and information sharing. Collaboration could also aid in foiling anticipated attacks and ease of tracking a suspected attacker.

- **Technology safety measures:** These include a wide range of technology enabled preventive devices and applications for combating cybercrimes. Examples include the use of antivirus software, use of security restriction features, monitoring features, and many more.

- **Personal safety Measures:** The safety of students (especially teenagers) from online dangers depends to a large extent on the individual concerned. Some of the literatures reviewed in this study shows that young people directly or indirectly orchestrates their vulnerability to online attacks. For instance, in a study to ascertain the effectiveness of security restriction features on certain perceived harmful sites in a particular school in Greece, Lazarinis (2010) revealed that the security features were unable to effectively prevent students who simply bypassed the applied security restrictions to access sites of their choice. It is therefore the responsibility of the students to put to use all the online safety tips they have been taught. In addition, it is also incumbent on them to be truthful, transparent and obedient to parents, guardians and teachers. They should also adhere to all instructions and guidelines given by parents, their schools or local councils, on the use of the internet.

- **Precautionary measures**: Online security like physical security, cannot be achieved by conventional means alone, individuals are still expected to take certain safety precautions to ensure more safety. The following are some precautions that could further enhance online safety for children and young people. Thus, parents, guardians and teachers should ensure that their children, wards or students should:

- minimize online presence especially when the child is alone;
- minimize posting online their pictures, houses, Cars, vacations, etc;
- avoid giving out their passwords to friends;
- avoid giving out personal details such as home or school addresses, phone, emails and other details to unknown persons;
- avoid chatting with unknown persons;
- decline physical meetings with unknown online friends;
- Use trusted educational sites like Khan Academy in engaging children in online learning;
- Use asynchronous learning more than synchronous learning for children and young people using the internet for e-learning purpose; etc.

Conclusion

This study reviewed literatures on online threats facing children and young people using the internet for educational and other recreational activities. Although cyber-attacks on children and young people have existed, the study found that these attacks increased greatly during the Covid-19 global lockdown as a result of increased online participations by many students globally (Zakuan&Saian, 2022; Mitra, 2020; Ahmad, 2020). The study also identified among other things some negative impact of cybercrimes on minors, some common causes and sources of attacks as well as some safety measures used in combating cyber-attacks.

Some of the commonly cited cyber-safety measures include development and implementation of cyber policy documents, security restriction features, parental safety measures, collaborative safety measures, the use of antivirus, among others. These measures though very usefully (Lazarinis, 2010) but still have some weaknesses identified with some of them. For instance, exploring the impact of using legal approach to combat cybercrimes, Zakuan andSaian (2022) reveals that though legal means is currently the main instrument used for the prevention of cybercrime in most countries of the world, it has not been found to be effective in combating cyber-bullying.In their study of cyber-safety policies in the United Arab Emirates (UAE), Siyam andHussain (2021) reported that all the policy documents on cyber-safety failed to address other cybercrimes and safety issues expect cyber-bullying.

In a study to ascertain the effectiveness of security restrictive features on certain perceived harmful sites in computer laboratories school in Greece, Lazarinis (2010) revealed that "the security features were unable to effectively prevent students who simple bypassed the applied security restrictions to access sites of their choice". Extensive studies on the role of parents in protecting their children against cybercrimes have also been carried by many researchers. While parents involvement are consider to be the most important and effective approach for combating cybercrime (Alqahtani, 2016; Moreno 2013), it was however reported that parents lack sufficient digital skills and knowledge to provide the needed supervision required to fully protect their children from online attacks (Alqahtani, 2016; Mitra, 2020).

In the light of the above, it is obvious that most of the conventionally identified measures of combating cybercrimes are not adequate to offer total protection to children and young people from cybercrimes. This call for additional precautionary and proactive approaches on the part of the stakeholders to minimizing cyber-attacks on minors as mentioned earlier in one of the sections above (online protection measures).

Emphasis on collaborative online safety measure is gaining global acceptance as a very effective cyber safety approach for children and young people using the internet (Mitra, 2020).Alqahtani(2016) posits that parents, teachers, the student and the government have a lot of role to play in ensuring online safety of school children. This implies that online safety requires a lot of efforts and it is the collective responsibility of all stakeholders.Therefore, synergy between all the stakeholders is required in ensuring greater online safety for children and young people using the internet, especially as attention towards online learning is on the increase due to the menace of the covid-19 pandemic and fear of similar dangers in future.

It is important to state here that despite the weakness identified with some of the safety measure above, a combination of all or some of them are desirable in ensuring online safety for children and young people using the internet, with emphasis on collaborative efforts among all stakeholders.

Lastly, from the literature reviewed, researches that addresses the issue of online safety, particularly during the covid-19 pandemic lockdown for school children learning online were mainly from the developed countries and the Gulf states with non from developing countries like Nigeria. Invariable there could be several cases of cybercrimes affecting young people from this clime without adequate attention from parents, teachers, government and scholars. This could be catastrophic for our nation if urgent attention is not paid to online safety for our children and young people as the demand for e-learning and other internet based activities is fast increasing.

Recommendations

- Parents should acquire digital knowledge and skills on cybercrimes and cyber-safety adequate to provide the needed online safety to their kids;
- Children and young people should be well educated on proper online behaviours (netiquette);
- There should be more advocacies and researches on the activities of cybercrimes and its impact on e-learning in developing countries such as Nigeria;
- Government and NGOs should create a website in Nigeria similar to Cyber Tiplineof the U.S where cyber exploitation or cyber-attacks on children should be reported. This will help the law enforcement agencies and other agencies to act promptly;
- Government should ensure that every school have a legal cyber safety policy in place before commencing online learning in their schools as it obtained in in the U.S and the U.K;
- There should be regular seminars/trainings/workshops on cyber-safety for students, school teachers, parents and communities to be organized by government, schools and non-governmental organizations;
- Pre-programmed digital learning devices such as the Eko Excel initiative of the Lagos state government should be encouraged and pursued by the Federal& other state governments.

References

Adelakun, I. S. (2020). Coronavirus (COVID-19) and Nigerian education system: Impacts, management, responses, and way forward. *Education Journal*, 3(4).https://doi.org/10.31058/j.edu.2020.34009. Retrieved from https://www.researchgate.net/publication/344115847_Coronavirus_COVID19_and_Nigerian_Education_System_Impacts_Management_Responses_and_Way_Forward

Ahmad T. (2020). Corona Virus (COVID-19) Pandemic and work from home: Challenges of Cybercrimes and Cyber security.*Social Science Research Network electronic journal.*https://doi.org/10.2139/ssrn.3568830.

Alqahtani, A. M. (2016). Keeping Safe Online: Perceptions of Gulf Adolescents.*Journal of Education and e-learning research*, 3(4), 150-155. Doi:10.20448/journal.509/2016.3.4/509.4.150.155

Chalmers, C., Campbell,M. A., Spears, B. A., Butler, D., Cross, D., Slee,P.,&Kift, S. (2016) School policies on bullying and cyberbullying:Perspectives across three Australian states. [Absract].Educational Research,58, 91–109.https://doi.org/10.1080/00131881.2015.1129114

Chen,Y&He, W. (2013) Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning.14(5):108-127 DOI:10.19173/irrodl.v14i5.1632

Edwards, S. (2021). Cyber-safety and COVID-19 in the early years: A research agenda. *Journal of Early Childhood Research*, 2021, 19(3), 396–410. DOI: 10.1177/1476718X211014908

Ezeamalu, B. (2012, August 22). How we raped, killed Cynthia, suspects in murder of General's daughter confess. *Premium Times.*Retrieved from https://www.premiumtimesng.com/news/97417-how-we-raped-killed-cynthia-suspects-in-murder-of-generals-daughter-confess.html

Farrukh, A., Sadwick,R., & Villasenor, J. (2014). Youth Internet Safety: Risks, Responses and Research Recommendations. Centre for Technology Innovations at Brookings. Retrieved 13th October, 2022 from https://www.brookings.edu/wp-content/uploads/2016/06/youth-internet-safety_v07.pdf

Lazarinis, F. (2010) Online risks obstructing safeinternet access for students. Technological Educational Institute of Mesolonghi, Mesolonghi, Greece.[Abstract]Retrieve from https://www.researchgate.net/publication/220677183_Online_risks_obstructing_safe_internet_access_for_students

Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child internet safety policy. ZER Journal of Communication Studies, 18 (35). pp. 13-28. Retrieved from https://www.researchgate.net/publication/285900088_Online_risk_harm_and_vulnerability_Reflections_on_the_evidence_base_for_child_internet_safety_policy

Machimbarrena, J.M., Calvete, E., Fernandez-Gonzalez, L., Alvarez-Bardon, A., Alvarez- Fernandez, L. & Gonzalez-Cabrera, J. (2018).Internet Risks: An Overview of Victimization in Cyberbullying, Cyber Dating Abuse, Sexting, Online Grooming and Problematic Internet Use. *International Journal of Environmental Research and Public Health*, 15(11): 2471. doi: 10.3390/ijerph15112471

Mark, L.K & Nguyen, T.T.T (2017).An invitation to Internet safety and ethics: School and family collaboration.*Journal of Invitational Theory and Practice*, 23(2017), 62-75. Retrieved 12th September, 2022 from https://files.eric.ed.gov/fulltext/EJ1184559.pdf

Mascheroni, G. &Ólafsson, K. (2014). Net children go mobile: risks and opportunities. Second edition. Technical Report · DOI: 10.13140/RG.2.1.3590.8561

Mishra, A., Alzoubi, Y.I., Gill, A.Q., & Anwar, M.J. (2022).Cybersecurity Enterprises Policies. A comparative study Published online. Doi: 10.3390/s22020538

Mitra, D. (2020). Keeping children safe online: A literature review. Centr for Excellence in Child and Family Welfare Melbourne, Australia. Retrieved from https://www.researchgate.net/publication/347442389_Keeping_children_safe_online_A_literature_review

Moreno, M.A., Egan, K.G., Bare, K., Young, H.N. & Cox, E.D. (2013). Internet safety education for youth: stakeholder perspectives *BMC Public Health* 13, 543 (2013). https://doi.org/10.1186/1471-2458-13-543https://www.researchgate.net/publication/237058603_Internet_safety_education_for_youth_Stakeholder_perspectives

Siyam, N. &Hussain, M (2021). Cyber-Safety Policy Elements in the Era of Online Learning: A Content Analysis of Policies in the UAE. *Association for Educational Communications & Technology*.http://doi.org/10.1007/s11528-021-00595-8 https://link.springer.com/article/10.1007/s11528-021-00595-8

Zakuan, Z.Z.M. &Saian, R. (2022). Cyber bullying victimization during COVID-19 Psychological effects and the legal measures. [Abstract]. *International Journal of Public Health Science,*11(1), 232-239. DOI: 10.11591/ijphs.v11i1.21047