A Study On The Cyber Safety Of High School Students During the Pandemic In Ernakulam

MASTER OF ARTS

Project Report

Submitted by

MARIA PAUL & SM20JMC013

Under the guidance of

TIJO K GEORGE

In partial fulfilment of requirements for award of the degree of

MASTEER of Arts

ST. TERESA'S COLLEGE (AUTONOMOUS), ERNAKULA

COLLEGE WITH POTENTIAL FOR EXCELLENCE

Accredited by NAAC with 'A++' Grade

Affiliated to

MAHATMA GANDHI UNIVERSITY

Kottayam- 686560

March 2022

DECLARATION

I do affirm that the project **“A Study On The Cyber Safety Of High School Students During the Pandemic In Ernakulam”** submitted in partial fulfillment of the requirement for the award of the Bachelor of Arts degree in English Literature and Communication Studies has not previously formed the basis for the award of any degree, diploma, fellowship or any other similar title or recognition.

Ernakulam

Maria Paul ,SM20JMC013

Masters in Mass Communication and Journalism

Department of Communicative English

CERTIFICATE

This is to certify that the dissertation titled, '**A Study On The Cyber Safety Of High School Students During the Pandemic In Ernakulam**' prepared and submitted by Maria Paul in partial fulfilment for the requirements for the award of the degree of **Master of Arts in Journalism and Mass Communication** is a bonafide record of project work done by the student and is hereby accepted.

Remya

Ernakulam

25 March 2022

Ms Remya John
Head of the Department,
Department of Communicative English.

CERTIFICATE

I hereby certify that this project entitled **“A Study On The Cyber Safety Of High School Students During the Pandemic In Ernakulam” by Maria Paul** is a record of bonafide work carried out by her under my supervision and guidance.

ACKNOWLEDGEMENT

I take this opportunity to offer my humble prayers and thanks to God Almighty for his mercy and blessings for the completion of this project.

I am deeply grateful to **Rev. Sr. Emeline CSST,** Director, , St. Teresa's College (Autonomous), Ernakulam **Rev. Dr. Sr. Vinitha CSST Provincial Superior, Manager**, St. Teresa's College (Autonomous), Ernakulam, for their kind cooperation and I am highly indebted to **Dr. Lizzy Mathew**, Principal, St. Teresa's College (Autonomous), Ernakulam, for her unconditional support and encouragement during my course of study in this institution.

I express my sincere gratitude to **Ms. Remya John**, Head of the Department of Communicative English, St. Teresa's College (Autonomous) for the valuable suggestions and guidance provided by her in fulfilling this project. I am profoundly indebted to my guide for her constant support and help for the successful completion of this project.

I am extremely thankful to my supervising guide, **name**, Department of Communicative English for his guidance and for all the teachers of the department for their valuable help rendered for the successful completion of this project.

Last but not the least, I wish to express my gratitude to my friends and family for their love and support.

Maria Paul

TABLE OF CONTENTS

CONTENTS

LIST OF FIGURES

ABSTRACT

Covid- 19 pandemic had urged sectors all over the world to evolve and adapt to safer and convenient modes of communication. Especially the educational system was completely altered in to the online mode of learning, forcing students of all ages to access the digital lessons every day. Whereas this setting has led to increased screen time among school children, leading to increased online harms like cyber bullying and sexual exploitation. This research aims to calculate the knowledge children have about cybercrimes and safety rules. This study is carried out among 100 high-school students, to analyse their cyber safety , along with a number of factors like transparency and the impact of impact. A structured questionnaire and interview method is been implied to understand the data better. This study is conducted in the Aluva division of the Ernakulam district.

A Study On The Cyber Safety Of High School Students During the Pandemic In Ernakulam

Chapter -1

INTRODUCTION

The Global Pandemic brought in copious amounts of uncertainties to the human race. Interpersonal communication is the basic and the most impacted aspect of all elements of human existence, during the outbreak of Covid-19. New approaches to life, emotionally, intellectually, and technically became the narrowed down solution for survival. To execute social distancing and safety norms all sorts of corporate and casual communications were refashioned through technology. The educational sphere as a whole had to maintain online coexistence with its crowd. According to UNICEF, 188 countries carried out school closures in 2020 impacting 90% of the student population. This altered the academic experience of the majority as well led to a 50% rise in internet usage among school goers.

Easy access to the internet and technology facilities comfortable learning space and platforms to socialize, but it also puts them into precariousness online. The Global Threat Assessment conducted by WePROTECT Global Alliance in collaboration with New York Times reported the relatively heightened probability of children being preyed on for online sexual exploitation during the epidemic. Cyberbullying, Hate Culture, and Discrimination are the menaces that commonly exist in online platforms, which can have negative impacts on juveniles. Children below the age of 13 happened to be less exposed to cyberspace before the pandemic, thereof the shortfall of interpersonal communication causes the ‘risk-taking behaviour’ to grow. Being exposed to harmful content online and left unmonitored can induce self-harm, suicide, or even inject violence in them.

1.1 Cyber Safety

Cyber security is the technical term for protecting computers, mobile devices, and networks against harmful threats. It can take many forms, including network, application, information, and operational security. The comprehensive approach to protecting children online through cyber security is to safeguard them from various hazards and assaults that they may face online. Cyber security enables us to use the Internet effectively for learning and communicating with those around. Furthermore, it is significant since it covers everything related to preserving our personal data, including sensitive data such as bank account information, proprietary information, and many others.

Children, especially the adolescents are steered with interest to know and explore the different dimensions of the cyber-world. Lack of knowledge about the possible traps and menaces in the internet space can lead into danger of multiple types. Children who are ignorant of the need of privacy protection and discretion may share personal images and videos. Such information might get into the wrong hands, leading to unlawful conduct such as online or physical crimes.

1.2 Cyber Threats Faced by Children

Some of the common threats in the cyberspace faced by children can be categorised into the following:

- Online transaction fraud - Majority of the youngsters do not have their own bank accounts. They do, however, commonly utilize their parents' accounts for online activities such as gaming, shopping, and so on. Fraudsters utilize a variety of deceptive strategies, such as contacting to offer user perks while using a false identity, to steal money from bank accounts.
- Cyber Bullying - It is the use of rude or abusive language to harass youngsters. This may be done by sending harmful content to them. Moreover, it can significantly undermine a child's self - esteem. It is crucial to know that if cyber-bullying of a child is not detected

early enough, it can have much further repercussions.

- Online Grooming - This is a method used to create an emotional bond with the child, through social media, gaming websites and others and develops a sense of trust in the relationship. After a period of time, as the child's faith in the impostor grows, the imposter gains the capacity to exploit the youngster and use him or her for his or her own advantage.

1.3 Keeping Children Safe

Before engaging in online activity, internet safety must be discussed with your children and must create an online safety plan. Parents must stablish clear standards, train them to recognize red signs, and promote open dialogue. Monitoring young child's internet use, including reviewing their profiles and postings on a regular basis are indeed inevitable. Electronic gadgets must be kept in open, common parts of the home and there should always be a thought about limiting their use. Before allowing children to download or use games, apps, or social networking sites, all of those should be subjected thorough review. Paying special attention to applications and websites that offer end-to-end encryption, direct messaging, video chats, file uploads, and user anonymity can help increase the maintenance of healthy boundaries for the children, as these features are regularly used by online child predators.

Using parental controls to adjust privacy settings for online games, apps, social networking sites, and electronic gadgets can keep the online activities of children in check. Informing children not to share personal information, images, or videos in public forums or with individuals they do not know in person, is also another effective way to teach them the ways to keep confidentiality. Children must be given proper explanations about the content that they publish online, which will remain in the web indefinitely. Educating children about bodily safety and limits, as well as the value of saying "no" to inappropriate demands in both the actual and virtual worlds can be added to list of measures to keep them safe. Changes in children's usage of electronic devices, attempts to conceal online activity, withdrawn behaviour, furious outbursts, anxiety, and despair are all potential symptoms of abuse, parents must always keep an eye of alert to analyse their children’s internet security.

1.4 Need for the Study

Reports (The Hindu, June 24, 2020) state that the number of child abuse cases reported with the Child-line in Ernakulam district progressively increased during lockdown. Kerala police Project Proposal 5 cybercrime stats also denote a remarkable increase in the rate of cybercrimes since the beginning of the pandemic. (Times of India, dec 24, 2021) Youngsters' online involvement is on the rise, as 232 million of India's 749 million internet users are children. The internet is a two-edged sword, allowing for connectedness, access to information, and entertainment on one hand, while also exposing users to potentially dangerous and improper content on the other. As sensitive and impressionable persons, children must be shielded against the negative effects of internet use. Cyber-bullying, cyber sexual harassment, cyber grooming, data breach, and the temptation to unlawful action are just a few of the risks. Because a rising number of children use social media to document and share their lives through images and videos, specific policies and processes are required to monitor children's online activities, limit risks and vulnerabilities, and safeguard them from damage.

Keeping the above context in mind, it has become essential to ponder on how much the young generation of today’s are aware of the potential cyber breaches they could be facing. Furthermore, once victimized, the experience becomes very hard on them that they restrain from confronting the situation, opening up, and reaching out for help. Unlike the earlier times, children are proximate to make more intelligent choices, and thereof would it have an impact on their cyber security. But the uncanny and abrupt rise in cybercrimes during the pandemic has made had us see the cyber world through the eyes of suspicion.

1.5 Objectives of the Study

The objectives of the study encompasses the following:

1) To analyse the cyber safety of children.

2) To determine the impact pandemic had on cyberspace activities of the children

3) To study the transparency children has regarding their experiences in the cyberspace

1.6 Research Questions

The study aims to focus on the importance of cyber safety awareness among high school students by draw out conclusions to the following questions

Q1) How much aware are the students about cyber safety measures?

Q2) How much have the online activities among students increased during the pandemic?

Q3) How willing are the students to seek for help?

Q4) What are factors that affect the willingness of the students to seek help and share their experiences ?

Chapter - 2

REVIEW OF LITERATURE

(Shakti, S., & Dhanoa, R. n.d.) Along with its benefits, the internet has exposed us to security concerns. Computers are now being abused for malicious operations like e-mail espionage, virus transmission, credit card fraud, spam, software piracy, and other activities that breach our privacy and outrage our sensibilities. Criminal activity on the internet is increasing, especially during these times of pandemic. The different types of cybercrimes that is active in today’s arena includes, hacking, cyber stalking, dissemination of obscene content, propagation of viruses, defamation, cheating, phishing, spoofing etc.

Information Technology Act, was passed by the Indian government in the year 2000. This act was adopted in order to effectively manage and oversee the activities of the cyber world. This act's Chapter 1X deals with offences/crimes, as well as a few additional provisions dispersed throughout the act. The following are the many offences covered by this chapter:

- Tampering with Computer source documents in Sec.65
- Hacking with Computer systems, Data alteration in Sec.66
- Publishing obscene information in Sec.67
- Unauthorized access to protected system in Sec.70
- Breach of Confidentiality and Privacy in Sec.72

- Publishing false digital signature certificates in Sec.73

(UNICEF. (2020). COVID-19 and its implications for protecting children online. Technical note, UNICEF and partners, New York.) Article published under the lead of UNICEF says that COVID-19 has resulted in extensive school cancellations and physical separation, making online platforms and groups important for resuming routine. Children and their families are using digital solutions to enhance their learning, socializing, and play more than ever before. While digital solutions provide tremendous potential for preserving and advancing children's rights, they also have the potential to increase the dangers to children on digital platforms. Online sexual exploitation, cyberbullying, access to hazardous information, incorrect data gathering, usage, and sharing, and inadequate child safety online are only a few of the significant challenges mentioned. This article also emphasizes the need of empowering, supporting, and promoting children's cyber safety and security practices

2.1 Cyber Crime Awareness

(Swamy, D. (n.d.). *AWARENESS OF CYBER CRIME AMONG TEENAGERS*. 3.) A study conducted to analyse the understanding of cybercrime among teens who access internet states that the majority of youngsters engage in cybercrime without realizing it, in other words most of the youth have poorer grasp of what a cybercrime is. For the investigation, 80 samples were chosen, 40 adolescent boys and 40 adolescent girls. To perform the work, Dr. S. Rajasekar's structured questionnaire was utilized. The attempted to state relations better the two variables, which were gender and cybercrime awareness. Nevertheless, the sample size did not favour a clear assumption, despite the differences in the awareness levels.

(Cyber Crime Awareness among College Students in Mangalore. (n.d.). Journal of Forensic Sciences, 6.) On examining the prevalence of cybercrimes among Mangalore university students by concentrating on varied threats, researchers found that there is a huge disparity in the amount of awareness of cyber safety among various fields. When compared to other subjects, science students show a high degree of awareness. The study was carried out using a survey method and included the UG and PG students of the Mangalore university as the sample or the research participants. This research process embarked the significance of awareness as a tactic for reducing/preventing cybercrime.

(Senthilkumar, K., & Easwaramoorthy, S.2017) With the evaluation of the cyber security awareness amongst Tamil Nadu college students by emphasizing on numerous security hazards on the internet, the statistics prove that, college students in Tamil Nadu have an above-average degree of awareness of cyber-related safety problems, which can assist them in protecting themselves from cyber attacks. Fully developed cyber awareness will teach kids how to defend themselves from hackers, therefore awareness must be raised to a higher degree. An organized questionnaire method was employed to conduct surveys in Tamil Nadu's main cities, concentrating on different security concerns such as email, malware, phishing, bogus advertisement, pop-up windows, and other online assaults. This poll helped the researcher study college students' comprehension and level of awareness of security concerns.

2.2 Impact on Children

(Babvey, P., Capela, F., Cappa, C., Lipizzi, C., Petrowski, N., & Ramirez-Marquez, J. 2021). Researchers state that the abrupt changes the society had to undergo during the pandemic have catalysed a surge in violence against children, specifically in the digital platforms. Excessive exposure to online platforms has made children subject to harmful content and cyber attacks. Thereof a study was conducted using the data collected from active social media users. Two main focuses of the study included the subjugation faced by children due to lack of interpersonal communication and menaces online like cyber-bullying, and the harmful information they were exposed to through the course of time. The study findings showcased the rise in the number of abusive posts and violence-inducing testimonials in social media. Thereof it is also recommended to empower families to protect 2 children, maintain online activities, and support services that work towards preventing online violence against children.

(Drane, C. F., Vernon, L., & O'Shea, S. 2021). It is important to have an assessment of the extent to which children are exposed to the usage of gadgets, especially during the pandemic. Full school closures were implemented in Australia over a lengthy period of time and a considerable number of pupils from more vulnerable backgrounds faced chronic disadvantage due to a variety of barriers: long-term educational disengagement, digital marginalization, ineffective technology management, and increasing psychological problems. Among these disparities, the digital divide decides the advancing of cyber threats among students. Socio educational backgrounds, availability of financial resources, access to the internet, and knowledge to advantage from the technology draw a fine line betwixt the possibility of someone being a victim. According to researchers, this study conducted before the invention of the COVID-19 vaccine corroborates the existence of factors that partitioned the access of students to online learning during the epidemic.

(Ma, W., & Mckinnon, T. 2020) Findings claim that COVID-19 has had a substantial influence on psychological and mental health in addition to changing people's general behaviour. Thereof cyber criminals prey on victims' psychological weaknesses, exploiting COVID-19- related fear and manipulating emotional instabilities to perpetrate cybercrime. Using psychological and classical criminological theories, this study investigates cyber fraud victimization and cyber security concerns during COVID-19. It also includes a cyber fraud taxonomy based on COVID-19 and empirical data from institutional and agency reports, aimed at providing classification insights to researchers and industry experts by arranging COVID-19- themed cyber fraud into four categories, so that stakeholders may better manage increasing cyber fraud threats in our contemporary pandemic. This aspect directly points out the problem that children are vulnerable, naïve and unprepared to face such atrocities online, thereof the need to keep them aware and awake is high on demand

2.3 Impact of Pandemic

(Jayakumar, P., Brohi, S. N., & Zaman, N. n.d.) On observing the destructive patterns that arose on behalf of the pandemic, the researchers concluded that aside from the loss of so many lives, it has resulted in a slew of issues, including unemployment, social isolation, business interruption, and everyday life disturbance. Those who live on the edge face even more difficult circumstances. COVID-19 has compelled mankind to develop and deploy alternate means to support enterprises and life within three months of its arrival. Researchers discovered seven lessons from the COVID-19 epidemic according to this report. Business, 4 education, online presence, network communication, cybersecurity, healthcare, and the meaning of life are among the sectors of assessment that are said to bear the impact. An asylum against cyber threats has been proved inevitable as almost every important function in the world has transitioned into its digital form.

(Eisner, M. A. N. U. E. L., & Nivette, A. 2020). According to the study, violence has a parallel relationship to the lockdown. The response to the pandemic has had an impact on a number of causal mechanisms that are essential to micro, meso, and macro theories of violence (see table below). These include the transformation of routine activity patterns and the consequences for patterns of face-to-face encounters; the disappearance of some violence related opportunity patterns, such as unsupervised time for teenagers, and the emergence of others, such as poorly protected targets for a property crime or home-bound victims in intimate partnerships; and an increase in violence-potentiating emotions and psychological states—anxiety, anger, and fear—as a result of the unwanted presence of others

(Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. 2021) The study states that the transpired sequence of cyber safety threats that came about as a result of the pandemic has to be subjected to scrutiny. This study uses the method of time-line analysis to examine the COVID-19 pandemic through the lens of cybercrime, emphasizing the wide range of cybercrimes that occurred worldwide during the pandemic. The modus operandi of cyber-attack campaigns is revealed by analysing and considering cyber-attacks in the context of major world events. Following what appeared to be enormous gaps between the first breakout of the pandemic in China and the first COVID-19- related cyber attack, the study indicates how assaults gradually became considerably more common, to the point where three or four separate cyber-attacks were recorded on certain days. Following that, the report uses the United Kingdom as a case study to show how cyber-criminals used important events and official pronouncements to meticulously plan and design cyber-crime operations.

(Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. 2021) This study examines cybercrimes documented in UK between May 2019 and May 2020 to see whether there has been a heightening in the case numbers as the lockdown and social distancing were enforced. The findings testify that the complaints of cybercrime surged during the COVID-19 epidemic, and they were especially high during the two months when the most stringent lockdown rules and procedures were in place. The number of occurrences linked with online shopping and auctions, as well as hacking of social media and email, which are the two most prevalent cybercrime categories in the UK, have increased the most. Individual victims, rather than organizations, have been the primary victims of the rise in 6 cyber-related crimes. This phenomenon places an urge to contemplate and target cyberspace where young adults are indulged in.

2.4 Applied Resolutions

(Bhatia, A., Fabbri, C., Cerna-Turoff, I., Turner, E., Lokot, M., Warria, A., Tuladhar, S., Tanton, C., Knight, L., Lees, S., Cislaghi, B., Bhabha, J., Peterman, A., Guedes, A., & Devries, K. 2021) According to this study, the Covid-19 pandemic has inflicted children with domestic violence, societal pressure, and online harm. The pandemic has shifted the spaces where the children spend time, from communities and the public to spaces online, which has led to a rise in online bullying, harassment, and child rights violations. The pandemic thus remains a milestone to remind the government, civil society, and communities to invest in enhancing child safety and addressing violence against children. The research suggests seven INSPIRE strategies and highlights the opportunities, the current scenario has created for us to act upon the child rights violations. The study also points out the importance of research and evidence to execute measures of prevention. Apart from these, the involvement of children and adolescents is given as important as well to bring in effective data collection and evaluation. These measures are expected to be effective even after the pandemic.

(Jevremovic, A., Veinovic, M., Cabarkapa, M., Krstic, M., Chorbev, I., Dimitrovski, I., Garcia, N., Pombo, N., & Stojmenovic, M. 2021) Researchers state that the school closures and social distancing approaches have cut short the children's time to interact in person. This phenomenon is potentially a reason for them to connect with third parties, who are unknown to them. Unmonitored interaction and sharing of information with such individuals can cause a threat to the children on multiple grounds. Thus, the need to keep children safe is essential, and the aids to help the process is highly indispensable in today's world. The existing software that works on child protection online, utilizes the limited information from the forbidden URLs to restrict activity. Thereof they had come up with a better system that scrutinizes contents, using techniques to determine to explicit nature of images, audio, and text to analyse whether it is neutral or harmful for the children. This highly complex framework examines Human-Computer Interaction (HCI) in real-time. This approach gave birth to the idea of Children's Agents for Secure and Privacy Enhanced Reaction (CASPER) to support and encourage child safety in online platforms. Moreover, the distinction and deletion of information that is harmful to children are given vitality throughout the study. The researchers have invested in deep learning techniques for image, audio, and text processing so as to distinguish visual content as pornographic or neutral, and textual content cyber-bullying or neutral.

(Okereafor, K., & Adelaiye, O. 2020) According to this study, the persistent dependence on digital platforms to curb the obstacle of social disengagement has paved the way to the rise of cyber-attacks, especially in the form of email scams, misinformation, harmful software inbuilt with viruses, and alike. as a result of this applied research, a solution was drawn out, which is the Randomized Cyberattack Simulation Model (RCSM) that helps keep track of the cybercrimes and tackle them. Researches also define this model as an example to attain cyber security in post pandemic cyberspace. The key drive that triggers cyber threats is the people's behavioural approaches in reaching out to information online. This indirectly demands a closer look at the intentions and perspectives of the audience. 5 Cyber attackers seemingly focus on this part to indulge in the act. This study came up with conclusions after analysing a number of cyber breach incidents and their effect on data privacy, accessibility, availability, and integrity

2.5 Identified gaps in the literature

Many researchers has studied the aspects of cyber crime, cyber safety, the impact of the pandemic and the extend of cybercrime awareness. The transparency of the children was hardly in focus for many of these studies. The abstinence from reporting cybercrimes , or safety breaches completely omits them from the desired population of majority of the researchers. The factors that impact children's willingness to interact for help thus is an area that needs to be given a certain amount of importance. Adolescent population, as stated in the researches, should be studied of their awareness of cyber safety in much gravity, as the chances for them being exposed to greater magnitude of internet space in the near future is substantially high.

Chapter - 3

METHODOLOGY

3.1 Introduction

This chapter deals with the features of research methods implied to conduct this research. Further in the reading, the author explains the research design (qualitative and quantitative), sampling methods, population and the sample, data collection methods and the tools used for data collected.

3.2 Research Design

Since the research is intending to access levels of cyber security awareness among high school students at the first part, a quantitative approach was adopted to serve the purpose. Along side, the impact pandemic had on the activities of children in the cyber space is also measured with the help of a quantitative approach too. Whereas studying the factors influencing the transparency and help seeking patterns of the high school children, demanded a deep observation and which was carried out with the help of a qualitative method of study.

3.2.1 Quantitative Approach

Cyber security awareness, especially during this later half of the 21st century among the adolescent age group holds much importance. The author implied a strategy that could help take into the account the first hand and unrefined version of information that can be absorbed for the selected population. To conform to the strategy, the samples were provided with questionnaire, accompanied with a brief orientation of survey method. The information the confined in this approach is mainly focused upon measuring the amount of cybercrime experiences and amount the safety methods they imply in their day to day life. In the second category of the study, the differences in time of usage of gadgets before and after the pandemic are the variables used for measurement.

3.2.2 Qualitative Approach

Qualitative approach is basically applied to assimilate descriptive answers, about a construct that potentially has a wide ground for study. In the context of this study, the researcher to preferred to engage in deep conversation with a relatively small and resonant sample and study the dimensions of transparency of the students. This method helped attain insight on the factors that affects the willingness of students of share their experiences and seek help.

3.3 Sampling Method

Multiple levels of sampling methods were used to develop the desired sample finalised for the study. As the target population was high school students in Ernakulam, it was inevitable to consider the number of schools in an around the location. Schools in Ernakulam are divided into four divisions, which are Aluva, Ernakulam, Muvattupuzha and Kothamagalam. The Aluva division was chosen using convenience sampling. At the next level, the author implied quota sampling, diving the schools based on the syllabus they follow(STATE syllabus and CBSE syllabus), from which two schools were selected to represented each syllabus. Later on the students between the ages of 13 to 16 were chosen through convenience sampling from the two schools. The sampling methods practised in all the levels belong to the category of non- probability sampling techniques.

3.4 Population, Sample and Sample Size

Understanding the composition of cyber affairs among the growing generation of our society helps us analyse and undertake initiatives to improve the conditions and refine the advantages of the cyberspace. There is also a rising concern of youngsters being victims of traps and threats online. Especially children at the brim of transitioning from being monitored by elders into exercising their independence in the usage of technology needs greater attention. Therefore, the population chosen to conduct this study was the high school students in Ernakulam. There are 88 government schools, 178 privately aided schools and 57 unaided schools under the four divisions of district Educational Officer in Ernakulam.. Of all these schools, two schools were to represent the STATE syllabus and CBSE syllabus respectively as the sampling frame. Both these syllabi are known to be the prominent in the district. The sampling size was narrowed down to a hundred students, 50 students from each of the two schools. Students belonged to the age group of 13-16.

3.5 Data Collection Methods

To the three objectives, the study was categorized into three sections, of which the first one was to collection data that would help analyses the cyber security, and awareness of the students. The second was to seek the impact of the pandemic in the cyber affairs of the students and the third to study their transparency. Combining all the three aims required the author to adopt three phases of data collection, analysis and investigation.

3.5.1 Phase 1

Phase 1 of the study included investigation of the sample frame and understanding the composition, attitudes and response of the sample. In this phase, authorities of each of schools were informed of the procedure and thereby permissions to conduct the study was obtained at this phase.

3.5.2 Phase 2

In the phase 2, questionnaires were distributed and alongside interviews were conducted with the selected number of students to study the patterns of transparency, the third category of the study. The data needed for the first and second category of the study was obtained from the questions incorporated in the questionnaires

3.5.3 Phase 3

Phase 3 was the time for collection of the data, i.e., the questionnaires that were distributed to the students selected from both schools. The collected data was combined and organized in order to analyse the proposed aspects of the survey.

3.6 Data Collection Tools

To conduct qualitative and quantitative study, interviews and survey methods were used respectively.For the interview, the selected number of 12 students were called in from each of the two schools. The students were interviewed one by one and were asked 5 different questions concerning the seeking help patters and transparency in sharing experience. Their answers were noted down to analyse the repetitions and diversity of perspectives, respecting their individuality .

A survey method was also implemented alongside the data collection process during the phase 3 of the study. A questionnaire containing about 13 questions was distributed among the selected 100 students, i.e, the sample. The data collected from the survey method was used to analyse and interpret the cyber of the sample using counter method and interpretations of the findings.

Chapter- 4

DATA ANALYSIS AND INTERPRETATION

4.1 Presentation of Data

The purpose of this study was to analyse the cyber security of students by exploring three dimensions of, namely cyber safety awareness, impact of pandemic on the cyberspace affairs of the children and finally the transparency of the students in sharing their experiences and seeking help. Prior to evaluating and understanding the core data, it is vital to not a few basic information about the sample, which includes composition of the sample and their alliance with technology and internet.

4.1.2 Demographics of the sample

The sample consisted of a total of 100 high school students of which 53% of them where females and 47% were males. Also the distribution of age according to the data recorded says that 25% of the population were 13 years old, 28% of the population were 14 yeas old, 23% of the population were 15 years old and 24% of the population were 16 years old.

Figure 4.1.2.1 Gender distribution

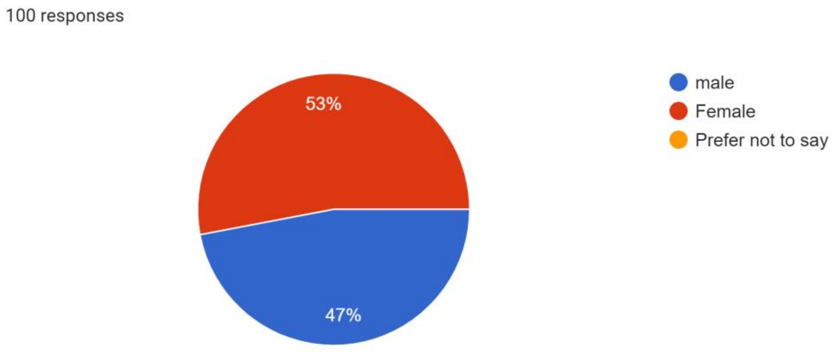
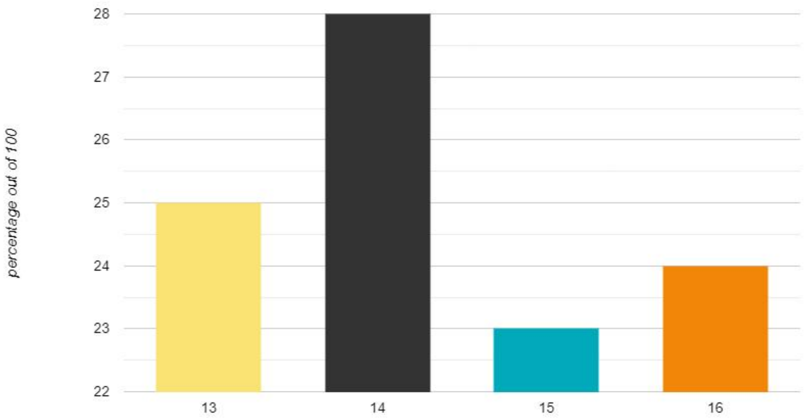


Figure 4.1.2..2 Age distribution

100 response



4.1.3 Technology and Access

Before understanding the extend of cyber safety awareness, it is inevitable to understand the correlation of how the access and usage of technology is distributed among the sample. To understand this three aspects are taken into consideration, which the type of technology students are given access to, the purpose of their usage and the extend of parental monitoring they receive whilst consumption of internet. According to collected information, 82% have access to television, 67% have access to computers, 35% have access to tablets, 82% have access to phones and 43% have access to laptops.

41% of the sample admitted that they are monitored sometimes, whereas 39% of the students use their gadgets under surveillance majority of the time. 2% of the children admitted that they are not at monitored by their parents while the consumption of internet and related technology. 10% of the students admitted that they rarely are under the monitoring of their parents and 8% confirmed that they submit to parent surveillance all the time, when accessing internet and related gadgets.

When asked about the purpose of usage of internet, 92% of the students utilize the facility to engage is connecting to their friends, 20% of them utilized it to gain knowledge or read articles, 62% of the sample used internet to help themselves with their school work, 92% used it to water video contents and 8% of them utilized the facility to play games, to entertain themselves with fan fiction, watch movies.

Figure 4.1.3.1 Access to Gadgets

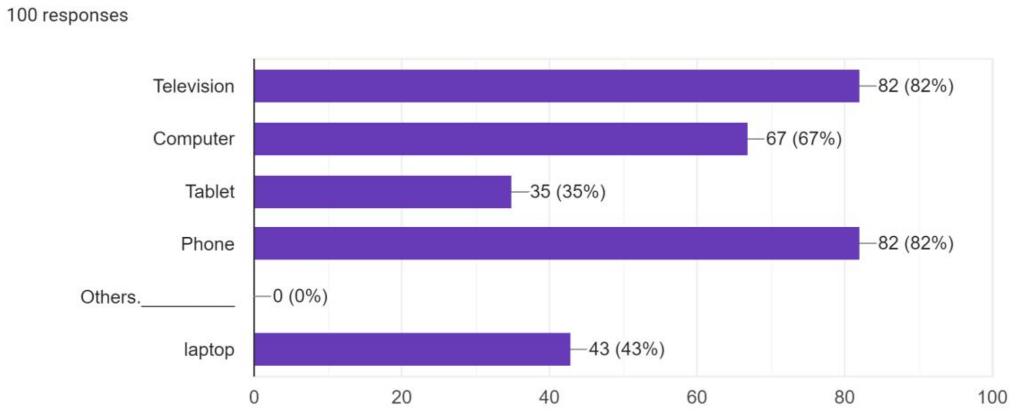


Figure 4.1.3.2 Parent Monitoring

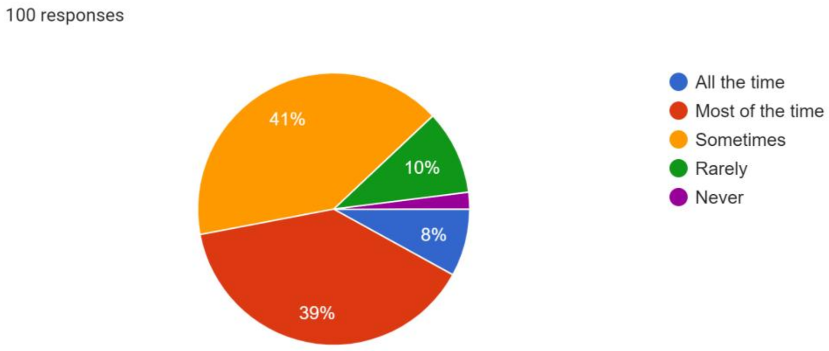
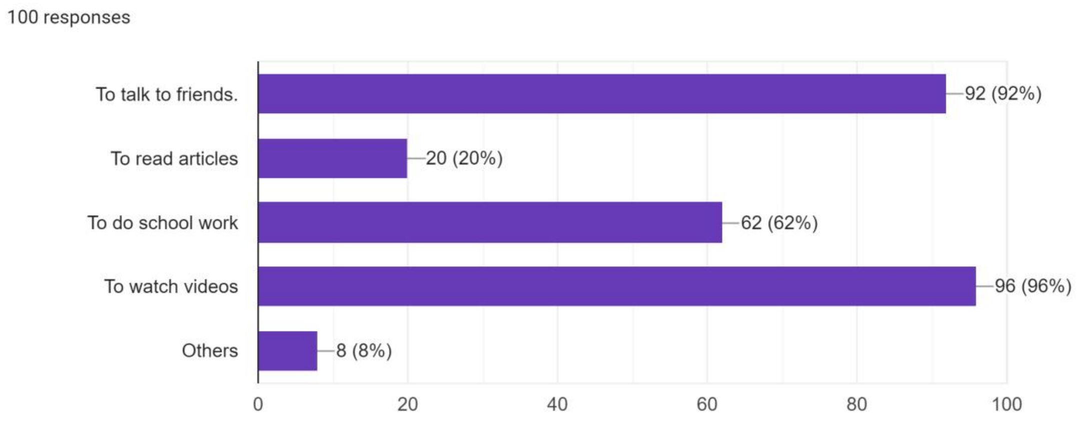
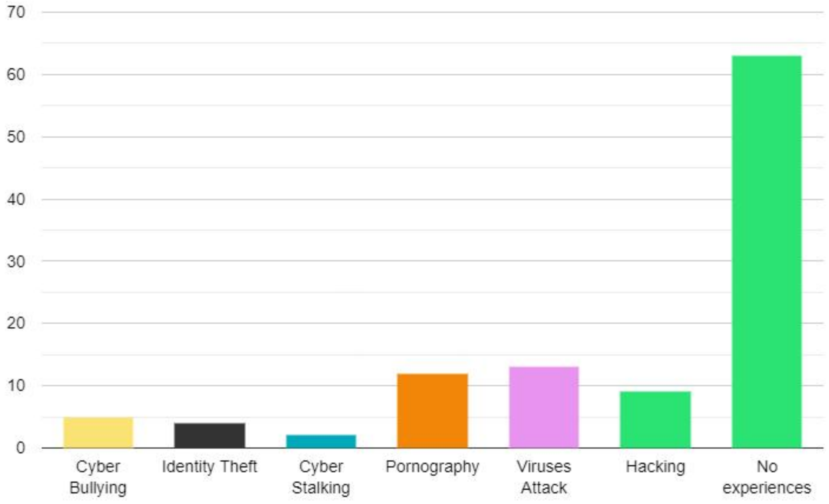


Figure 4.1.3.3 Purpose of Usage



4.1.4 Cyber Crime- Victimized Experiences

Figure 4.1.4.1 Cybercrime Experiences

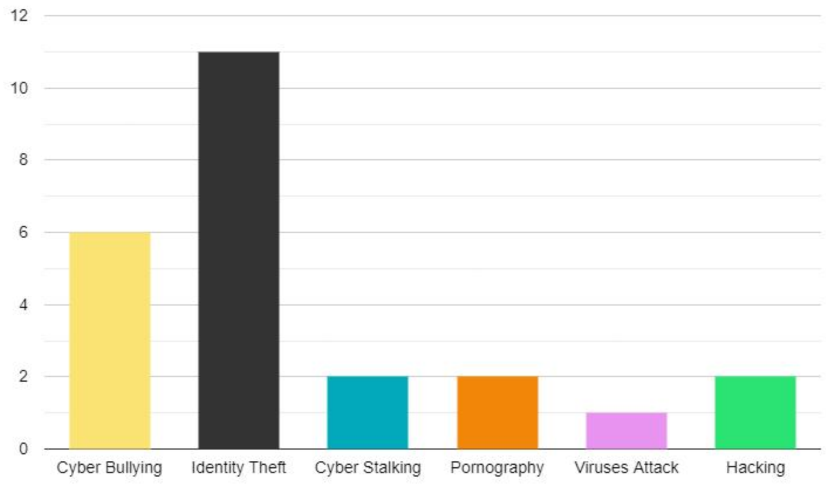


One way to analyse the awareness of the cyber safety is by evaluating the cyber crimes they have experienced through their lifetime. 5% of the students admitted they are had been cyber-bullied at the course of their internet usage. 4% of the sample confirmed that they have experienced identity theft, especially in the social media platforms, 2% of the students reported that they have experienced cyber stalking, 12% of the population confirmed that they were sent sexual content by someone older than themselves, 13% had come across viruses attack in their devices, 9% of the population confirmed them being a victim of hacking and 4% of the population reported cyber frauds and money looting. Where of the entire population 63% of them agreed that they've never been a victim cyber crimes done against themselves.

4.1.5 Cyber Crime-Committing Behaviour

On the interrogation of behaviours that leads to cyber crimes, 6% admitted that they have cyber bullied others, 11% agreed that they partook in identity theft, mainly by creating social media accounts in the names of others, 2% admitted that they did cyber stalking, 2% had sent sexual content to someone of their age, 1% admitted the creation of virus attack and 2% partook in hacking.

Figure 4.1.5.1 Cybercrime Committing Behaviour



4.1.6 Application of Safety Measures

The students were asked of the safety measures they undertook whilst accessing internet. 65% of the students have installed anti-virus software in their devices, 30% of students had deleted their social media accounts, 50% of them reduced the amount of information they post of the public platforms, 34% of them limited the number of audience to their social media posts, 34% reviewed and reinforces the security systems they utilize, 64% of the students only visited websites that are deemed to be safe, 27% used different passwords to secure their information on various gadgets, platforms and social media, 69% only open emails from trust-able sources and 63% limited their social media visibility to people they know.

4.1.7 Impact of Pandemic on Online Activities

To measure the amount of time students had been investing into before and through the pandemic, students were asked of the time periods of consumption of the internet before the pandemic. In accordance with the days before the pandemic, 77% stated that their consumption of internet happened only once or twice a day and the reasons to which were the regular classes they had to attend. 16% said that they used the internet only couple of times a week, 5% access to the internet only couple of times a month and 2% stated that they did not use at all.The statistics of the data collected of the internet usage states that, 56% of the students spent more than 6 hours using the internet, 25% of them spent 5-6 hours, 15% of them spent 3-4 hours and 4 percent of them spent 1-2 hours.

In a specific question about the impact, Internet usage during the pandemic, has had on the students, 42% of them said that the usage of internet has helped them gain knowledge, 7% of the students admitted that it has put them into danger, 78% of pointed out that it has affected their studies and 37% of them stated that they picked up addictions because of it.

Figure 4.1.6.1, Usage of Internet during the pandemic.

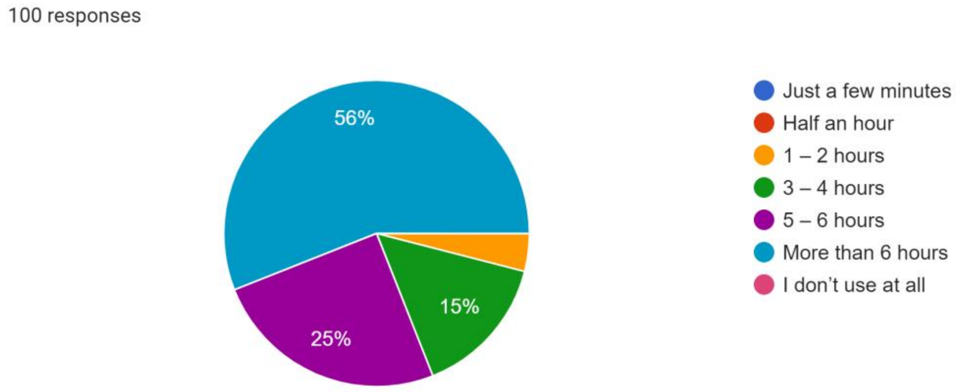
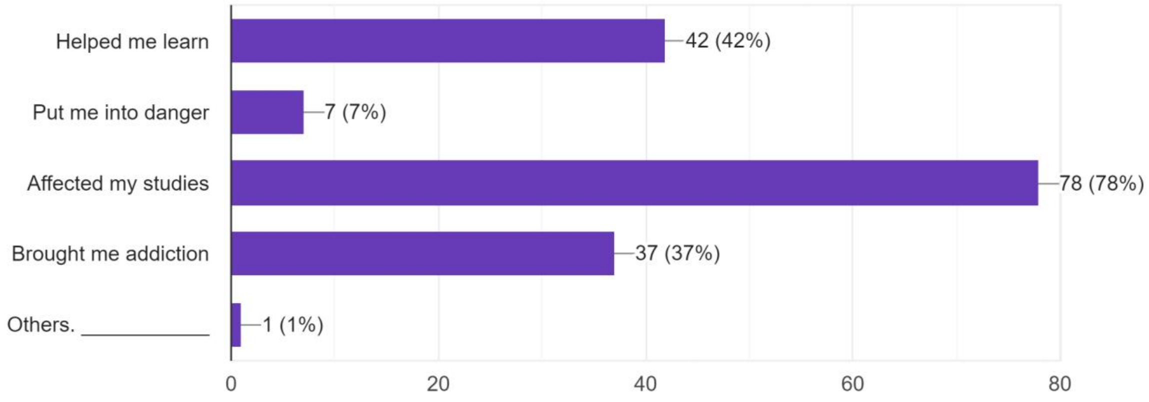
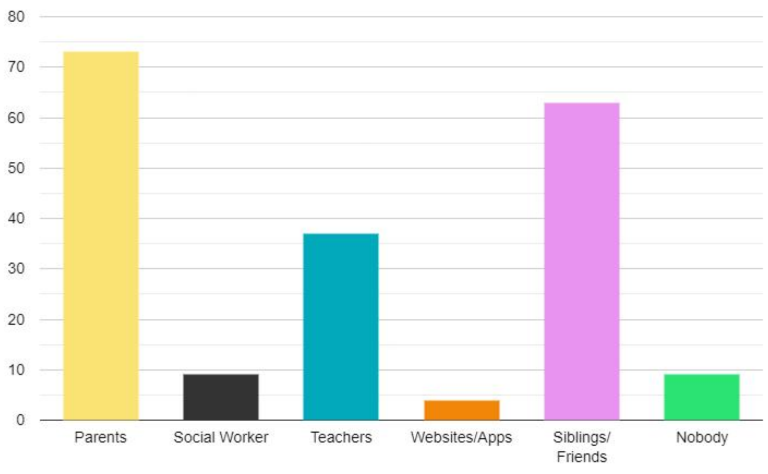


Figure 4.1.6.2 Impact of Pandemic



4.1.8 Transparency in Reporting and Seeking Help

Figure 4.1.8.1 Preference of Source to Seek Help



To learn the dimension of transparency in reporting the cyber crimes, students were interviewed of factors that affect their willingness to share their negative experiences, quotes such as ‘ I am afraid of being blamed', ‘ I will be scolded at’ and ‘they fail to understand me' repeatedly was brought about. On interviewing the sample, the author observed the reluctance of the students to share their fears about sharing was noted. There were also a few number of students who claimed to have no fear in reporting a crime that has happened to them or crimes they were involved in. 17 students among the sample, firmly said that they are not willing to share their experiences with anyone. When interrogated of their expectations of how their parents, teachers or person who can help should behave, the students used words such as comforting, motivating, understanding, safety feeling, accepting, supportive, calm, kind, patience and optimistic to explain the environment they expect at times of them needing help. The students were asked of their reactions if someone approaches them for help related to cyber threats. ‘Seeking help from elders', ‘ would report to the police', ‘would comfort them and listen' and ‘ I will help in ways I can' were the statements that were repeating through the interview. On the questions of whosoever they would consult in need of help in cyber safety, 78% of the students named their parents or guardians in charge, to seek help from, also 63% of the total students said that, they would go to their friends and siblings.

4.2 Discussion

This session establishes the connection between the obtain data and findings of the study, alongside evaluates the results in accordance with the objectives of the study. It was found than a good majority of the students have not been victimised to any of the cyber crimes and thus there are many factors that involves in keeping their safety in check

4.2.1 Cyber safety

On analysing the safety of student, 63% of the students were found to have experienced any cyber threats or traps and all of the students have exercised cyber safety measures according their knowledge. A maximum of 11% admitted their indulgence in cyber crimes as well. 50% of the students admitted that they need guidance to maintain their safety . The above data implies that, cyber safety and safety awareness of the students can be and is in need of improvement.

4.2.2 Impact of the Pandemic

The pandemic has made a huge rise in the amount of time students invest in the consumption of internet, moreover 78% of them confesses that this behaviour had negatively affected their studies. 37% of the students pointed out about addiction and obsession to the gadgets and cyber platforms. This data implies that, pandemic has adversely impacted majority of the students, thereof a careful consideration of reversing the effect has to be implemented to advantage the students.

4.2.3 Transparency and Seeking Help

The factors that influence the transparency of the students are the attitudes, responses and the consequences they have to face from the sources of their help. Overreaction and anger discourages the students of their hope to find help. Moreover the elders are accountable to offer help so that we can make the lives of our younger generation easier. The kind of response that that induces healing, mentally and physically would encourage our children to be transparent about their experiences .

4.3 Findings

From the overall data that had been collected, it was found that 41% of the students confessed of them under the monitoring of their parents and 78% of the students opted to reach-out their parents at times of cyber threats or related emergencies. This emphasises the role parents has in ensuring the safety of their children. The only factor that stands in between the procedure is the wrong approaches parents exercise to confront their children in matters of cybercrimes, traps or related problems. Especially during this period of pandemic, it is advised to adopt measures that improves the relationship of the children with them parents or responsible guardians.

Chapter - 5

CONCLUSION

This study was intended to study the cyber safety of the high school students and factors that relate to this. On understanding about the cyberspace experiences of the students, it was evident that majority of them have had information on cyber safety, whereas they admitted that they should be guided more to maintain their safety. Pandemic has increased the numbers if cyber crimes reported against children, because they have become exposed to the facility more than ever. Moreover, it has affected their studies, induced fears and brought on addictive behaviours. Here's where the authority figures have the role to play. The very proximate and available help for a child is their parents, siblings and friends. This study brought about conclusion that responsible entities must adopt health way of listening and understanding , when it comes to dealing with the matters of cyberspace with adolescent children.

5.1 Limitations of the study

The study was carried out during the times of Covid-19, thereof reaching out to the population with probability method of sampling was not favourable. This not only has impacted objectivity of the results, but also minimizes the diversity of responses that could have been possible to collect. The sample group were given the questionnaire to participate in the study from their own premises, which had led some of them into giving vague answers. Another fact includes the demographics of the sample. As a result of convenience sampling, the number of children are not equally distributed across the age groups and gender. Alongside, the observed reluctance of the children in being honest about their experiences adds up to the limitations of this study.

5.2 Suggestions for the Future

There are lot of opportunities in studying role of individuals in the life a child in maintaining cyber safety. A qualitative approach in he behavioural aspects of the parents that negatively impact children can bring in insight to better the lives of children. The factors that lead a child in to involving in cyber crime behaviours, would also add to safe keeping of the younger generation.

REFERENCES

1) Babvey, P., Capela, F., Cappa, C., Lipizzi, C., Petrowski, N., & Ramirez-Marquez, J. (2021). Using social media data for assessing children's exposure to violence during the COVID-19 pandemic. *Child abuse & neglect*, *116*(Pt 2), 104747. https://doi.org/10.1016/j.chiabu.2020.104747

2) Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering, 263, 042043. https://doi.org/10.1088/1757-899X/263/4/042043

3) de Silva, M. W. A. (2007). Child rights violations as seen by children. The Island Magazine.

4) Cyber Crime Awareness among College Students in Mangalore. (n.d.). Journal of Forensic Sciences, 6.

5) Joshi, A., & Kandpal, S. (2020). CYBER CRIME AWEARNESS AMONG ADOLESCENTS. 8(12), 8.

6) Shakti, S., & Dhanoa, R. (n.d.). International Journal in Multidisciplinary and Academic Research (SSIJMAR) Vol. 2, No. 2, March-April (ISSN 2278 – 5973). 7.

7) Rahman, M., Ahmed, R., Moitra, M., Damschroder, L., Brownson, R., Chorpita, B., Idele, P., Gohar, F., Huang, K. Y., Saxena, S., Lai, J., Peterson, S. S., Harper, G., McKay, M., Amugune, B., Esho, T., Ronen, K., Othieno, C., & Kumar, M. (2021). Mental Distress and Human Rights Violations During COVID-19: A Rapid Review of the Evidence Informing Rights, Mental Health Needs, and Public Policy Around Vulnerable Populations. Frontiers in Psychiatry, 11, 603875. https://doi.org/10.3389/fpsyt.2020.603875

8) Bhatia, A., Fabbri, C., Cerna-Turoff, I., Turner, E., Lokot, M., Warria, A., Tuladhar, S., Tanton, C., Knight, L., Lees, S., Cislaghi, B., Bhabha, J., Peterman, A., Guedes, A., & Devries, K. (2021). Violence against children during the COVID-19 pandemic. Bulletin of the World Health Organization, 99(10), 730–738. https://doi.org/10.2471/BLT.20.283051

9) Drane, C. F., Vernon, L., & O'Shea, S. (2021). Vulnerable learners in the age of COVID-19: A scoping review. The Australian Educational Researcher, 48(4), 585–604. https://doi.org/10.1007/s13384-020-00409-5

10) Ma, K. W. F., & McKinnon, T. (2022). COVID-19 and cyber fraud: Emerging threats during the pandemic. Journal of Financial Crime, 29(2), 433–446. https://doi.org/10.1108/JFC-01-2021-0016

11) Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, [102248]. https://doi.org/10.1016/j.cose.2021.102248

12) Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. Journal of Contemporary Criminal Justice, 37(4), 480–501. https://doi.org/10.1177/10439862211027986

13) Jevremovic, A., Veinovic, M., Cabarkapa, M., Krstic, M., Chorbev, I., Dimitrovski, I., Garcia, N., Pombo, N., & Stojmenovic, M. (2021). Keeping Children Safe Online With Limited Resources: Analyzing What is Seen and Heard. IEEE Access, 9, 132723–132732. https://doi.org/10.1109/ACCESS.2021.3114389

14) Okereafor, K., & Adelaiye, O. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. 05(07), 13.

APPENDIX

The following questions belong to the set of quantitative analysis survey:

1. Which of the following devices do you have access to?

a) Television

b) Computer

c) Tablet

d) Phone

e) Laptop

f) Others

2. How often do you use your gadgets under your parents monitoring?

a) All the time

b) Most of the time

c) Sometimes

d) Rarely

e) Never

3. What do you use the internet for?

a) To talk to friends

b) To read articles

c) To do school work

d) To watch videos

e) Others

4. How often had you been using the internet before pandemic?

a) Once or twice a day

b) Only a couple of times in a week

c) Very less in a month

d) I didn't use the internet at all

5. How much time did you use the internet in a day during pandemic?

a) Just a few minutes

b) Half an hour

c) 1 – 2 hours

d) 3 – 4 hours

e) 5 – 6 hours

f) More than 6 hours

g) I don't use at all

6. Exposure to internet during pandemic has :

a) Helped me learn

b) Put me into danger

c) Affected my studies

d) Brought me addiction

e) Others.

7. Please tell us if you've ever experienced any of the following:

a) I've been cyber-bullied

b) I've cyber-bullied someone else

c) Someone else has pretended to be me online

d) I've pretended to be someone else online

e) I have been tracking down someone online

f) I had been tracked by someone online

8. Please tell us if you've ever experienced any of the following:

a) I've sent messages with sexual content to someone about my age

b) Someone older or younger than me has sent me messages with sexual content

c) I've sent messages with sexual content to someone older or younger than me

d) Someone has shared or threatened to share sexual content or images of me online to try and get me to do something

e) I've had a virus or other harmful software on one of my devices

f) I've created a virus or other harmful software and distributed it online

g) Someone's hacked or tried to hack into my computer / device / online account

h) I've hacked or tried to hack into someone else's computer / device / online account

i) I've been the victim of a fraud online and lost money

j) I've carried out a fraud online and the other person lost money

9. Which of the following statements do you agree with?

a) 'I am safe in the cyber space'

b) 'I am afraid of being cyber attacked'

c) 'I am aware of the threats online'

d) 'I need guidance to improve my safety’

10. Which of the following actions have you ever taken to keep yourself safe online?

a) Installed anti-virus software on one or more of my devices

b) Deleted a social media application or account

c) Reduced the amount of personal information I disclose on my social media accounts

d) Limited who can see my posts on social media

e) Reviewed or changed the security settings on my browser / search engine

f) Only visited websites if I know and trust them

g) Used different passwords for different sites / apps

h) Updated my passwords

i) Only opened emails from people I know

j) Only opened attachments if I'm sure I know who it's from and what it is

k) Only accepted friend / chat requests from people I know

l) Prefer not to say

m) Others.

11. Where would you get helpful advice about staying safe online? Choose all that apply.

a) Parents or someone else who looks after you

b) Another person I trust

c) A social worker / support

d) worker

e) Teachers

f) Prefer not to say

g) Others

h) I would never ask for help

i) Websites or Apps

j) Siblings or Friends

k) The police

12. How willing are you to talk about your negative experience online?

a) Not willing at all

b) somewhat willing

c) wiling

d) very willing

e) prefer not to answer

The following questions are part the qualitative analysis interview.

13. Briefly explain your fears regarding opening up about a bad online experience to your parents.

14. How does the attitude of the source of help affect your honesty in sharing?

15. What is the kind of response you are expecting from your parents or teachers when your share your concerns, fears or experiences?

16. What are kinds of help would you be looking for when you approach ?

17. What would be your response when someone struggling with online issues approach for help to you?