Exploring and Improvising Cyber Security Awareness in Young Pakistani Children

By

Rabia Kalsoom

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Systems Engineering.

September 2021

CERTIFICATE

This is to certify that **NS Rabia Kalsoom** Student of **MS SYS ENGG-04** Course Reg.No **00000204616** has completed her MS Thesis title **"Exploring and Improvising Cyber Security Awareness in Young Pakistani Children"** under my supervision. I have reviewed her final thesis copy and satisfied with her work.

Thesis Supervisor

(Brig. Abdul Rauf, PhD)

Dated

Declaration

I certify that this research work titled "*Exploring and Improvising Cyber Security Awareness in Young Pakistani Children"* is my own work. The work has not been presented elsewhere for assessment. The material that has been used from other sources is properly acknowledged and referred.

Signature of Student

Rabia Kalsoom

00000204616

Dedication

This study is whole heartedly dedicated to my mother (May her soul rest in peace) and my father (May ALLAH grant him with good health), whose prayers always change all the difficulties into ease and to my beloved son and family for their untiring support

Acknowledgement

All praises to ALLAH Almighty, The Most Merciful, The Most Beneficent, Who gave me His countless blessings and courage to complete my thesis. After that I would like to express the deepest appreciation to my supervisor Brig. Abdul Rauf, PhD for his time, without his guidance, patience and persistent help this study would not have been possible. His constant support and encouragement helped me in bringing my research to the refined edge. I am also grateful to my worthy GEC members Major Muhammad Sohaib Khan and Assistant Prof. Dr. Fawad Khan for their timely help.

I am very grateful to my mother who always helped me and guided me throughout my life and motivated me to complete my thesis and my father Major Jahan Khan and brothers who always encouraged me to study hard by their support. I am grateful to all my sisters for their constant support and motivation. Special thanks to my brother Dr. Ahmad Ali Khan for being the pillar of my utmost strength and to my sister Tahira Fatima for always motivating me and guiding me throughout my educational career. Heartiest thanks to my Husband Malik Muhammad Yousaf for his untiring support and always staying by side till the end. I am also grateful to my beloved son Muhammad Farqaleet Yousaf, who is reason of my motivation. And special thanks to my friend Ayesha Areej who helped me in proof reading this write-up and my friend Rida Rashid who kept me motivated through this journey, and also a special thanks to the caretaker of my baby, Aunty Naheed, without her help I wouldn't be able to complete my thesis.

I express my heartiest thanks to all the friends and family members around who always showed concern to my academic career. At the end I am also grateful to all the respondents who participated of this survey based research study.

Abstract

ICT has become an essential part of our daily routine. Increase in internet-based services has given rise to opportunities as well as threats in cyber space. Young children are especially more vulnerable to online threats. Pakistan has a large number of internet users with maximum young people. Pakistan is one of the countries developing in the digital domain but generally lacking cyber awareness especially among children. Thus there is a need to create cyber awareness among its citizens and particularly among children. Some efforts are already taking place but there is a need to explore the shortcomings in this regard. One of the major steps in this regard could be introduction of ICT education with focus on cyber awareness into our national education curriculum. Purpose of this research is to explore present cyber security vulnerabilities, threats and awareness concerning children and young people in Pakistan, and to find the weak areas where improvements are required to enhance the overall cyber security awareness situation.

A thorough study about top internet risks has been done for this purpose and internet risk categorization has been taken place on the base of research. In the start of the research study, a survey has been designed according to internet risk categorization and conducted among a group of children via both offline and online means to get an overview of present cyber security awareness situation in children. After analyzing survey results, which shows the suffering of children in almost all the domains of cyber risks as 25% of the children have reported that they were disturbed most by the fake news spread on the internet. Second most reported category is Online Harassment which is one of the worst online risks. 21% of the children have reported this as having worst effects on young mind. At third place 14% of the targeted sample told that adult/violent content has most negative impact on their young minds 10% reported for both disclosure of personal data and for religious hatred and provincial bigotry. At last place 9% of the children reported bullying as the worst happening online risk to them. Training sessions have been organized for the group of children surveyed offline via paper based face to face questionnaire and tips to remain safe online are shared with online participants in form of a brochure.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1: INTRODUCTION

1.1 BRIEF DESCRIPTION

ICT has become an essential part of our daily routine. Increase in internet-based services has given rise to opportunities as well as threats in cyber space. Young children are especially more vulnerable to online threats [1]. Pakistan has a large number of internet users with maximum young people. Pakistan is one of the countries developing in the digital domain but generally lacking cyber awareness especially among children. Thus there is a need to create cyber awareness among its citizens and particularly among children. Some efforts are already taking place but there is a need to explore the shortcomings in this regard. One of the major steps in this regard could be introduction of ICT education with focus on cyber awareness into our national education curriculum. Purpose of this research is to explore present cyber security vulnerabilities, threats and awareness concerning children and young people in Pakistan, and to find the weak areas where improvement is required to enhance the overall cyber security awareness situation. For this purpose, a thorough study about top internet risks has been done and internet risk categorization has been taken place on the base of research. In the start of the research study, a survey has been designed according to internet risk categorization and conducted among a group of children via both offline and online means to get an overview of present cyber security awareness situation in children. After analyzing survey results training sessions have been organized for the group of children surveyed offline via paper based face to face questionnaire and tips to remain safe online are shared with online participants.

1.2 LEVEL OF RESEARCH ALREADY CARRIED OUT ON THE TOPIC

Cyber security has become the most-discussed topic worldwide in the context of expanding internet-based systems and networks and threats thereof. In Pakistan, although some researchers have analyzed threat scenarios and impact of cyber breaches [2] [3]. Critical services that can be future target of cyber criminals have been identified and some preventive measures have also been proposed [4] but unfortunately, till date, no serious research has been documented for safe usage of internet among children and young people. In the global context, especially among developed countries, children safety on the Internet is taken very serious and research is actively being carried out in this field. A UK based study shows that regardless of

expansion of internet access, parental fears, both technical (accidental downloading a virus, data loss, disabling a software) and social (social engineering, stalking, exploitation, and stranger danger) are impeding children's free online exploration. For this educational and awareness schemes have been developed [5]. Another study has classified the internet risks for children in three categories — content, contact, and conduct — and formulated a security awareness program [6]. US Department of Education had also published a report to help children to stay safe online while growing up in a digital age [7]. In Belgium a long-term study was conducted to introduce structured outline of internet risks and suggested ways to cultivate safe online behavior [8]. A survey has also been done of community stakeholders in Australia for online safety of children from negative impacts of cyber environment [9]. In context of primary and secondary schools in South Africa, a framework has been devised to develop an e-safety culture [1]. Even in India, E-safety situation has been analyzed for children [10]. Pakistan is lagging behind significantly in this field which should be a matter of concern for everyone.

1.3 SCOPE OF WORK

Reasons for the selection of Topic are as under:

1. Securing Cyber space is the most critical need of the era.
2. Children and young people are more vulnerable and prone to internet threats because of their unawareness of dangers lurking in cyber world.
3. Young children safety from online threats is necessary because more than 50% of our population is from the age group of under 19 years [11].
4. A definite generational gap exists between parents and children. Parents are mostly unaware of their children's online behavior and are unable to teach them how to remain safe online [12].
5. Awareness and education about cyber security among children and young people will play a vital part in promoting a cyber security culture in the nation and make it well prepared for future challenges.
6. Cyber security has huge importance as the future war fronts will be in cyber world.

Due to all above mentioned justifications the scope of this research has been clear. Above key points show that this research is a much needed domain and will be beneficial for children and all the other stakeholders i.e. parents, teachers and the state.

1.4 RESEARCH OBJECTIVES

The main objectives of thesis are:

1. To evaluate cyber security awareness among children in Pakistan
2. Defining the most vulnerable area of cyber risks for children in present cyber threat spectrum and its expansion in the coming era for young people
3. To gauge level of awareness about cyber security and make it generalize on all young children of the country

1.5 RELEVANCE TO NATIONAL AND ARMY NEEDS

Studies have shown that cyberspace is a new emerging domain of future warfare. The worst International cybersecurity breaches include Russian Cyber war against Georgia, US' cyber-attack against Iran to fail their nuclear program and the Russian hackers' cyber-attack against NATO. Pakistan is also facing similar threats [13] [3]. Some of the recent incidents include:-

1. Regularly defacement of websites, especially government websites by hackers
2. Careem data hack where a data of 14 million users was compromised from all over the world including Pakistan
3. FIA reported occurrence of hackers' attack on almost all Pakistani banks in 2018 where customers' data including debit/credit card data was compromised. This resulted financial losses through unsolicited transactions from accounts
4. WanaCry (Ransomware) attacks in 2017
5. Use of social media for promoting religious sectarianism and provincial bigotry is common nowadays

All these incidents and many others show very clear relevance of proposed topic with nation integration and security as children are the future of a nation. If we talk particularly of children, according to a report published by Kaspersky lab, the top most dangers that children face online worldwide are cyberbullying, cyber-exploitation, disclosing private information, being victim to scam offers, phishing, unintentionally downloading malware, and posts that come back to haunt a child life long [14]. Same is the case in Pakistan as UNICEF has warned about the expected threats caused by online violence, cyber bullying, and online harassment for majority of young online people of Pakistan and demanded to take firm preventive measures for online violence against children and young people [15]. As a huge number of children are getting access to cyber space and involved in online activities, the trending issue faced by them is cyberbullying [16]. Hence, it is very important to train the children to stay safe online so that they will be able to compete with cyber psychological threats of the future.

1.6 ADVANTAGES

Advantages of the research conducted are listed below:

1. Knowing weak points in Cyber Security Awareness level in young population of the country
2. Training young minds to remain safe online
3. Creating awareness for e-safety in schools and on online platforms

1.7 AREAS OF APPLICATION

Areas of application include primary and secondary school and college going children's cyber security awareness in Pakistan.

1.8 THESIS OVERVIEW

Chapter 1 **INTRODUCTION** briefly explains the aim of the study and the strategies to meet the research objectives along with describing the need of study and the background knowledge of the topic. This chapter also describes the relevance of the research taken out with the country needs.

Chapter 2 **LITERATURE REVIEW** describes different strategies taken by different nations to mitigate cyber sufferings of the children. It describes general threat land scape of Pakistan and how we are lagging behind in making our children aware of cyber threats lurking on internet.

Chapter 3 **RESEARCH METHODOLOGY** describes the survey life cycle from design and process perspective along with selection of mode of survey and detail description of internet risks categorization which are going to be measured in the survey questionnaire.

Chapter 4 **QUESTIONNAIRE DESIGN** describes the process of designing the questionnaire with construct specific response options to gauge awareness level in the domain of cyber security in young children of Pakistan.

Chapter 5 **RESULTS AND DISCUSSION** shows the findings and analysis done on the data gathered via online and offline survey along with meaningful discussion.

Chapter 6 **CONCLUSION** is the last chapter of study which concludes the whole study along with recommendations and future work.

Chapter 2: LITERATURE REVIEW

2.1 INTRODUCTION

The internet, although designed originally for information sharing only, now is the network of networks. As the world entwined increasingly and physical and cyber world are constantly merging, the cyber threat spectrum has also increased in breadth and depth. The inherent characteristics of internet and cyber world i.e. connectivity and globalism, are its most exploited vulnerabilities. Moreover it also has a design problem as security was never the concern of the initial developers which can be seen in seven layer of Open Systems Interconnection (OSI) reference model without a security layer. [10] However, simultaneous evolution of Internet and cyber world resulted in the advent of Artificial Intelligence (AI) and Internet of Things (IoT), the humans are now at the back seat to technology. The severity of cyber threats is not merely confined to loss of data, instead it is "a threat posed by use of digital device as a tool (for initiation or facilitation) or target, which if materialized can cause loss in data or information, money, critical system or even human life, "as indicated in Figure 1.

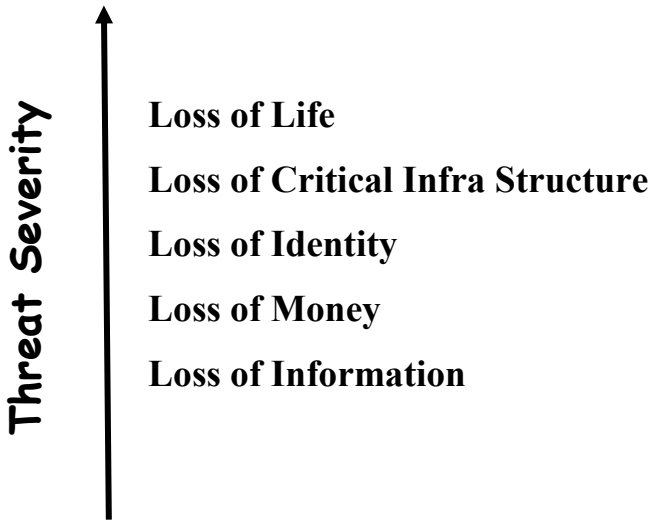


Figure 1: Internet Threat Spectrum

Gordon & Ford [11] Internet society's Global Internet Report-2017, indicates Cyber threats as one of the key factors – called 'Driver of Change' – that shapes future of internet [11]. In 2019 Data Breach Threat Investigation Report identifies financial gains as the main (71%) reason behind data compromises preceded by espionage; the reason behind 25% of the attacks. [12] Financial gains translated into strategic advantage was noticed in most infamous WannaCry ransomware attack of 2017 as well as the theft of $ 81 million from Central Bank of

Bangladesh, Dhaka in 2016. [14] Average figure of 145 security breaches in 2019 was 11% larger than preceding year with noticed 67% increase in last five years. [13] The most vulnerable targets were small and medium size businesses, which faces 43 % attacks followed by public sector institutions facing 16% attacks. [12] IBM reported a direct link between early threat identification and total average cost of that breach. [14] Annual financial loss of US $600 was observed in 2019 as compared to US $ 445 billion in 2017. [18] However, ever increasing digitalization in critical infrastructure and Internet of Things is putting human life at stack. The most notorious example is Stuxnet used against Iran, supposedly by US. The attacks on Ukrainian power grid by malicious program on Dec 23, 2015 open breakers to 30 sub stations resulting in power loss affecting 200,000 consumers. It is [15].The digital infrastructure in health care industry remained under continuous threat of cybercrimes, which may pose serious threat to human lives.

2.2 DEFINITIONS

Youth refers to persons having age less than 18 years [17].

Awareness campaigns means to promote such a culture of cyber security that can address the requirement of whole society [18].

The basic purpose behind cyber security awareness campaign is to make people adopt secure online behavior. NIST Special Publication defined security awareness as under: *"**Awareness** is not training. The aim of awareness presentations is to highlight the importance of security. Awareness presentations are aimed to allow individuals to recognize Cyber security concerns and act accordingly"* [19].

According to IST-Africa *"**Cyberspace** refers to a physical and non-physical territory created by and/or composed of some or all of these components: computers, networks, computer systems, computer data, traffic data, content data, computer programs, and the users"* [20].

The draft South African Government Gazette of South African National **Cybersecurity** Policy defines: "*illegal acts, performed by using information and communication technologies"* [20].

Cyber security is defined as*: "the collection of tools, security concepts, policies, guidelines, security safeguards, risk management approaches, training, actions, best practices, assurance and technologies that can be used as protection measure for the cyber environment, user assets and organization"* [20].

According to Ministry of Defense-Estonia ***"Cyber security awareness** is the security training that is used to motivate, stimulate, initiate and renovate skills relevant to cyber security and expected practices of the security from a specific audiences"* [20].

2.3 REASON BEHIND UNSAFE INTERNET USAGE

Lack of knowledge is considered as the most contributing factor in unsecure online behavior which is the major reason why awareness about cyber security is of utmost importance. In USA, to elevate the level of awareness in the nation on the risks linked with cyberspace is the main aim behind cyber-security education. In UK, the target is to help individuals and enterprises, by making them aware of cyber-security. And in Australia and Canada, the eventual goal is to promote cyber security culture by raising awareness [21].
Most of the parents of current generation were grown up before the emergence of World Wide Web (www). Due to this situation it is the responsibility of society to create awareness in children and young people to surf safe and remain aware of rangers lurking online [22].

2.4 CLASSIFICATION/ CATEGORIES

ITU (International Telecommunication Union) has devised rules and regulations by categorizing the minors in five categories on the basis of age groups. The first age group is of children between ages 2 to 4 years these are not able to think critically or do something on their own on internet. The second category is of the children aged 5-7 years they are also not able of critical thinking but can use internet for gaming purpose or entertainment. This make them vulnerable to commercial risks as paid subscription of games and contact risk as filling on line forms or feedback surveys. The third category is of children aged 8-10. They are more vulnerable to having contacts with unknown people and adults via social media and are also interested in gaming and internet surfing. The fifth and last category ranges the children

between ages 14-18, and are able to access all possibilities of internet and are hence vulnerable to all kind of online risks [17].

This paper [17] categorizes the risks on the basis of situations as well:

1. Online risks which leads to real life problems, e.g.; pornography.
2. Online risks which are consequence of interaction of two children e.g.; cyberbullying.
3. Online risks which are consequence of interaction of a child with an adult, e.g.; cyber exploitation.
4. Online risks which emerge by the unwanted collection of data by online forms, against the defense of privacy, for example viruses, worms and other malware.

Third categorization which is popular in the literature is on the basis of internet usage by the children. And these are content risks, contact risks and commercial risks. Further content risks can be separated in three sub domains: (a) illegal content e.g.; sexual assault (b) harmful or age inappropriate content e.g.; content based on hatred or violence and (c) harmful advice e.g.; content that may lead to consumption of drugs or suicide commitment. Similarly, Contact risks are further divided into (a) cyber grooming that occurs when an adult predator communicate online with a child and further seeks offline contact, (b) cyber bullying mostly occurs in online gaming platforms and social media, (c) cyber harassment differs from bullying as the contact is not in peers but between an adult and a child and (d) sharing of personal information e.g.; photos and addresses to unknown persons. This hugely possess to online privacy risks Commercials risks are described in two ways: (A) Children targeted as consumers for products or services targeted for adults e.g.; drugs or medicines. The ads for these products usually targeted the websites or pages made for children such as online games, and (B) Economic risks e.g.; fraudulent transactions or paid subscriptions of ring tones etc. [17].

A comparative study between cyber security awareness initiatives in a developed country, the UK, and a developing country, South Africa, categorizes the cyber risks in three main categories: (i) One's aim to harm the learner such as Cyber bullying: trolling (saying something controversial on social media to start quarrels), flaming (posting insults or using offensive language on social media), excluding (progressive social rupture and detaching from social relations), masquerading (identity theft or pretending to be someone which is not actually behind bullying), mobbing (a group of people involved in bullying and ganging up using rumors, isolating, false and usually malicious accusation and discrediting i.e. damaging the reputation), denigrating (criticizing and use of harmful and usually untrue statements), outing (leaking out personal chat etc. or reading personal messages), harassing, cyber grooming, impersonation (pretending to be another person while committing cyber harassment etc.),

blackmail, cyber snooping (unauthorized access to someone's data), identity theft, online predators, social engineering, etc. (ii) Learner's subjection to dangerous online contacts such as Inappropriate material/content, digital reputation ruin, chat rooms and social platforms, viruses, cookies, malware etc. (iii) Learner's unintentional involvement in dangerous situation such as plagiarism, illegal file sharing, free downloads, inappropriate posting online, non-ethical postings of others' material, copyright infringements, exploitation etc. [23].

In [24] cyber threats have been categorized in two categories. One that affects national sovereignty for example cyber terrorism and the other that includes traditional criminal wrongdoings such as, theft of intellectual property or sexual exploitation of young children.

It is important that school going children must understand their liability in safeguard themselves and their data/information online. Other cyber related problems to be coped with incorporate: managing privacy settings, protecting passwords, following cyber ethics age-appropriateness, meeting in real life people you initially met online, and digital footprint. School going children should be encouraged and furnished to take liability for their own cyber safety through effective awareness education and programs [23].

2.5 WORK DONE WORLDWIDE

Many international organizations and researchers are trying to study and categorized the dangers lurking online via conducting surveys, and recommending safety measures on the basis of survey findings. ITUs-Child Online Protection (COP), EU Kids Online, Net Children Go Mobile, Youth Protection Roundtable (YPRT) and many others are included [17].

South African Cyber Security Academic Alliance (SACSAA), the Digital Wildfires project in UK, Childnet and similar other projects are involved in cyber security training and education of young children in South Africa. Industry also play vital role in cyber security awareness as the Internet Safety Campaign (ISC) is initiated in South Africa, which has developed several online resources. Similarly, in the UK many projects like the UK Mobile Industry Crime Action Forum, Safer Internet Centre the and the TechFuture Partnership have been initiated. The difference between [23].

In Malaysia, a survey has been done among social networking users. The survey questions were categorized into three domains: (i) basic, (ii) technical, and (iii) advocacy. The survey results shown that there exist a huge difference in the level of awareness of the respondents on the basis of educational background and gender. It is evident from the survey that females and higher educated persons are more aware of cyber security [25].

In Macedonia, the government has started a program named e-Macedonia with primary goals: e-Government, e-Education, e-Citizens, e-Business, information security and infrastructure. This initiative have gave rise to both the opportunities as well as cyber threats to both state and non-state actors. In 2015, Macedonian government established a responsive team named Macedonian Computer Incident Response Team (MKD-CIRT). Bosnia, Serbia, and Herzegovina are also following same methodologies and approaches to create awareness in people like Macedonia. While many other countries like Albania, Bulgaria, and Croatia are much advance than before mentioned countries as they not only raise awareness campaigns but also give proper consideration to education to raise level of awareness to whole nation [18].

In UK, GetSafeOnline campaign was initiated to advice people to stay protected online, their selves along with their businesses. Similarly, The Cyber Streetwise Campaign in UK also focuses on individual users at home and their businesses and advise them to follow a five liner code i.e.; (i) using strong passwords, (ii) using antivirus softwares on their devices, (iii) enabling privacy settings on social network accounts, (iv) updating systems as soon as patches are available, and (v) checking retailer's security before uploading card details [19].

In Africa, a cyber security campaign named ISC Africa, intended to educate people to use internet and computers in safe and responsible manner. Similarly, another campaign there named, Parent's Corner Campaign, efforts to coordinate the work of all the three tiers of community, government, industry and civil society. It aims to protect and educate children and parents to beware of online risks and remain safe in digital world [19].

Cyber criminals enjoy four major benefits: anonymity, non-formulated boundaries of cyber space, 24/7 availability of internet, and indirect nature of cyber-attacks [20].

Cyber Security Awareness is a matter of prime concern in South Africa. It is evident from the initiatives taken there. Among these startups, University of Venda's and Council for Scientific Industrial Research (CSIR) initiative with target population as secondary schools, technical and non-technical university, education training colleges, , community centers, and support staff teachers/educators, initiative of University of Pretoria (UP) (ICSA- PumaScope) with target audience as schools in remote areas, churches, and orphan homes, initiative of University of Nelson Mandela Metropolitan (UNMM) (ISM) with targeted audience as general company end-users, entrepreneurs , children, parents, and senior citizens, initiative of University of Fort Hare (UFH) with target population as university students, University of South Africa (UNISA) with target audience as school students, South African Banking Risk Information Centre's (SABRIC) initiative with target audience as South African Bank employees, Information Security Group of Africa (ISG-Africa) targeting organizations and society, South Africa Centre

for Information Security (CIS) targeting organizations in all aspects, are worth mentioning [20] [21].

The National Initiative for Cyber-security Education (NICE), an organization in USA has been formed. In the UK, Get Safe Online, an external organization, deals with matters associated with cyber security education and awareness. In Australia, multiple governmental departments deal with cybersecurity awareness and education but this causes confusion in target audience about which source to trust. Public Safety Canada forms the focal point in cyber-security awareness and education [21].

Cyber security awareness catch a lot of focus in start of second decade of 21st century. ISO/IEC 270032, an international standard was published in 2012. It differentiate cyber security from other forms of security [26].

2.6 WORLDWIDE ADOPTED METHODOLOGIES

A comparison based study gives overview of the different initiatives and identify various sectors behind these initiatives that are government, industry, academia or educational institutions. The methodology adopted for this study revolves around review of existing initiatives in South Africa and the UK, including the literature available on internet along with digital and print media. The study critically analyze the existing initiatives in both countries, their purpose, and the driving sectors [23].

A survey has been done in Malaysia among social networking users to explore level of security awareness [25].

The technologies adopted in Macedonia are worth mentioning. The three major projects for creating awareness are briefly discussed here: (i) Children's Right on the Internet- Safe and Protected and Online Privacy Made Easy (CRISP): This campaign was initiated between 2007 and 2008 and aims to protect right of children in online digital world, to provide safe and secure online access, to protect online privacy of children and their families, raise campaigns to create awareness in primary and secondary schools, arrange trainings for children, their parents, guardians and teachers, publish posters and brochures containing awareness material, developed a website that provide free material and guidelines for online safety of children and their teachers and families. Moreover, Directorate of Personal Data Protection (DPDP) in Macedonia has developed a project named "Class for Privacy" having similar features as CRISP, but is more interactive in nature as it focused on games like mobile and online fraud, cyber bullying, securing passwords etc., videos and movies based on awareness, and

questionnaires regarding online data protection and privacy. The content associated with this project is noteworthy as it is based on true incidents occurred online, in chatting, through emails and social media. And last but not the least, this project offers "Safer Internet Day" on yearly basis in February. (ii) Surf Safe: This project was started in 2013 and its main focus is to identify threats and risks that lure online for children and young people, make people aware to stay away from fake profiles on social platforms and not to share personal stuff online to avoid exploitation later on, device a national strategy according to European Union's standard for better internet. The project has initiated a travelling caravan in collaboration with UNICEF and some other institutions. This caravan displayed awareness posters in native language, leaflets with additional awareness guidelines were distributed among teachers and parents. This caravan also distributed free activation keys for parental control software. One hour training named "I can hack your facebook… can you catch me?" was conducted to train people to discover intruders. (iii) Privatnost (Privacy): This project got started in 2015 and was aimed mainly in research direction for protection of citizen's individual privacy. It also provides visual presentation of analyzed laws, suggest amendments in laws that deal with privacy of citizens and provide awareness raising educational stuff on regular basis [18].

2.7 COMPARISON OF METHODOLOGIES

Different initiatives that have been taken in South Africa and UK in terms of cybersecurity are compared as under: (i) School curriculum is being organized by Academia in South Africa while in UK, government and industry do the job. (ii) Similarly school workbooks are being published by Academia in South Africa while government, industry and academia collectively do this task. (iii) Teacher's training is the field in which South Africa is lagging behind while government and industry are giving due concern to it in UK. (iv) School ICT policies and procedure are devised by both government and schools in South Africa while in UK only schools are responsible for this. (v) Incident handling process in schools has not been devised in both countries. (vi) In South Africa, awareness material e.g.; posters and brochures are designed by academia and Industry while in UK this project is being done by government and Industry. (vii) Only schools participate in parent involvement projects in South Africa while in UK both government and industry take part in it. (vii) One-off initiatives such as workshops, talks and open days for creating awareness are held by academia, industry and schools in South Africa while the same activities are being held by government and academia in UK. (viii & ix) Web presence as well as traditional media presence is monitored by industry, government and academia and by government and industry in South Africa and UK, respectively. (x)

Legislation, policy or regulation on cybersecurity in schools is done by government in both countries. Hence it is concluded that in UK government has taken noteworthy steps in creating awareness whereas in South Africa the vital role is played by Academia. Moreover, the cultural difference is also obvious from the initiatives for example UK's GetSafeOnline campaign shows that the focus is on individual efforts to remain safe while in South Africa the campaigns like Parent's Corner indicates that the emphasis is on collective approach [23].

2.8 DAMAGE CAUSED BY CYBER CRIMES

An overview of cyber security conditions in Muslim world, along with major cyber-attacks occurred worldwide, is discussed [24]. A malicious hacking group LulzSec- attacked Sony Pictures and took data including passwords, names, home addresses, email addresses and DOBs of thousands of people. Another attack occurred on services of foreign intelligence and 24,000 files have been stolen from pentagon defense contractor. An attack has occurred on PlayStation of Sony Company and consequently they face a loss of $171 million. In Muslim world, the Stuxnet infection targeted the uranium improvement project of Iranian Nuclear program. This attack was done by US. A series of Saudi Arabian government websites were targeted and consequently crashed due to Denial-of-Service (DOS) attack controlled from unknown location. In 2012, a computer virus named "Shamoon" attacked computer network of Aramco, a Saudi Arabian Company of Oil and Gas. This virus infected about 30.000 work stations. The responsibility was claimed by a group named "Cutting Sword of Justice". Several websites of UAE banks war targeted by phishing attacks, in January 2010. Several customers in UAE lost their bank savings, in April 2010, due to online fraud attacks. The hackers extend the cash amount and credit card limit in National Bank of Ras Al Khaimah and Bank Muscat of Oman, and causes a damage of $ 45 million from both [24].

Damaged caused by cyber-crimes in South Africa is briefly discussed in [20]. According to this study, 16 pc of total cyber-crimes victims were affected through their own cell phones in South Africa as compared to global statistics, which is 10 pc only. Majority proportion of cyber-crime consist of computer viruses and malware and rest is made up of phishing fraud and scam. The total loss faced by South Africa due to cyber-crime is about R10.9 billion till 2011, which is approximately 1 pc of the global loss which is estimated at R2.9 trillion [20].

2.9 WORK DONE IN PAKISTAN

Cyber security has become the most-discussed topic worldwide in the context of expanding internet-based systems and networks and threats thereof. In Pakistan, although some

researchers have analyzed threat scenarios and impact of cyber breaches [2] [3]. Critical services that can be future target of cyber criminals have been identified and some preventive measures have also been proposed [4] but unfortunately, till date, no serious research has been documented for safe usage of internet among children and young people. In the global context, especially among developed countries, children safety on the Internet is taken very serious and research is actively being carried out in this field. A UK based study shows that regardless of expansion of internet access, parental fears, both technical (accidental downloading a virus, data loss, disabling a software) and social (social engineering, stalking, exploitation, and stranger danger) are impeding children's free online exploration. For this educational and awareness schemes have been developed [5]. Another study has classified the internet risks for children in three categories — content, contact, and conduct — and formulated a security awareness program [6]. US Department of Education had also published a report to help children to stay safe online while growing up in a digital age [7]. In Belgium a long-term study was conducted to introduce structured outline of internet risks and suggested ways to cultivate safe online behavior [8]. A survey has also been done of community stakeholders in Australia for online safety of children from negative impacts of cyber environment [9]. In context of primary and secondary schools in South Africa, a framework has been devised to develop an e-safety culture [1]. Even in India, E-safety situation has been analyzed for children [10]. Pakistan is lagging behind significantly in this field which should be a matter of concern for everyone.

2.10 DRAWBACKS/SHORTCOMINGS

Pakistan is lagging behind in this field. This is prime responsibility of the state, the educational sector and the parents collectively to make the children of Pakistan aware of the threats lurking on internet and to teach them how to remain safe online.

Chapter 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION AND OVERVIEW

The aim of this chapter is to provide an overview of the problem statement and main goal of this research. The scope of research is to increase awareness of Cyber Security concept and its importance among youth of Pakistan. The main purpose is to explore this concept explicitly to assist in educating young children regarding the severity of being well-aware of consequences associated with sharing data online. The study falls in following three research areas:

1. Descriptive – which includes statistical study in the form of means or percentages subgroups (just members) will be studied and calculated.
2. Predictive – this section will cover weather forecast etc.
3. Casual – which includes gathering data for some cause.

From all these categories i.e., descriptive, causal, and predictive our research scope is confined to Causal category. As, the purpose of this research is to explore the level of awareness in our young generation about the threats lurking on internet. The study will include a survey in which data will be collected regarding the awareness level of students about main categories of risks faced by children online for further analysis. These risk categories include content risks, contact risks, commercial risks and conduct risks. For survey, all the four categories were divided into further subdomains based on which questionnaire was designed, ensuring a validate data collection. Afterwards, the survey was conducted with family members and friends and collected feedback to understand the validity and accuracy of the drafted questionnaire. The questionnaire was further improved based on the feedback and quality of data collected from initial target group because the main difficulty participants experienced was of understanding technical terms used in the survey. It was alleviated by adding simple definitions of such terms. Meanings in Urdu Language were also added for difficult terminologies and the questionnaire was finalized in such a way that everyone who has least knowledge even no knowledge of cyber threats can easily understand and answer these questions.

3.2 RESEARCH/MEASUREMENT OBJECTIVE

The objective of this research is to measure the awareness level of Young Pakistanis via conducting a survey. Commonly, the inferential goals from a survey are to generalize it on a larger population, in a larger time frame and in a larger geographical area that holds the survey results. However, the scope of this study was confined to online survey method instead of face-to-face surveys or interviews. Hence, the sampling frame is supposed to be random, and the

inference is more general. To explore the awareness level of whole young population of Pakistan was not achievable in the given time frame and research limitations. Therefore, an online survey was conducted via social media and different online schooling platforms and through the help of friends, family, and colleagues, and collected responses from different cities all over the country. Therefore, the results will infer on general youth of the country. Meanwhile, an interviewer also administered face to face survey on a smaller scale in public sector institution of Islamabad capital territory in a limited time, due to COVID pandemic situation. The purpose for conducting this offline survey was to check the validity of our online survey by comparing the results for both. So that reliability of the research can be maintained, along with achieving inferential goal. An overview of the objectives of this research are listed below:

1. To gauge level of awareness about cyber threats in young generation of Pakistan via conducting an online survey.
2. Inferring the survey results to general children population of Pakistan.
3. Conducting an offline survey on minor level to validate the authenticity of first survey.
4. Comparison of both surveys to meet our inferential goal in a better way.
5. To improvise the cyber security level of awareness up to some extent.

3.3 CONCEPTUAL OVERVIEW/FRAMEWORK

As mentioned above, the aim of this research is to achieve inferential goal through the survey to gauge awareness level of youth of Pakistan. So, the key ingredients for valid inference must be kept in mind and the data must be generated in such a way that it must infer target population correctly i.e., the results can be generalized to all. Therefore, the survey must be generalized to all younger population out there in Pakistan. For this purpose, following factors were considered:

1. Data generating process must be finalized prior to conducting survey.
2. A framework must be derived to identify errors in generated data.
3. Eliminate all ambiguities associated with research scope and goal. More specifically, it should be very clear from the beginning that what kind of results are needed that means confounding factors must be identified beforehand.
4. Inferential goal must be well-defined.
5. Research questions should be clearly and precisely defined.

3.4 MEASUREMENT AND ANALYSIS PLAN

There are two types of reasoning processes which includes the deductive reasoning and the other is inductive reasoning. For both processes, different modules and classification of data have been introduced. For example, (a) Found data, also known as organic data, and (b) Designed data. Furthermore, for both types, prior understanding of data generating process is essential and without having a clear research question and specific hypothesis in mind it is very difficult to achieve your inferential goals from the gathered data.

To closely align the problem statement/research question with the scope it is important to design the research questions. Hence, for planning what is needed? The following points hold significant importance:

1. What is specific research question?
2. What are expected results?
3. Have all the aspects of research question been covered or not?
4. Have all the concepts been translated into measurements/questions or not?

First step is the research objective which is defined as "*Exploring Cyber Security Awareness in Young Population of Pakistan*".

Second step is the expected outcome and for this study that is basic level of awareness about the threats lurking on internet is expected. The reason behind this is little to no access to mobile devices in majority of children in Pakistan and the IT course including in Pakistani curriculum hardly covers the information and mitigation strategies about the online threats.

Third step is to cover all the aspects of research topic. For this purpose, detailed research on the categorization of internet risks has been carried out. According to survey data generating process, explained in Figure 1, it is termed as constructs followed by the Figure 2 which explains the construct flow chart. After thorough studies, the internet risks have been classified in two domains (a) Human risks and (b) Technological risks. Further these categories are divided in sub domains and finally the constructs.

Finally, these constructs are converted into measurements/ questions, through which awareness level can be measured. For this several questions related to each subcategory of every construct has been designed and a questionnaire has been collated which is appended at the end in Appendix A. To make the questionnaire more comprehensive, simplified explanation of difficult terms were added along with Urdu translation of security related so that majority of participants can easily understand and respond accurately. Furthermore, Table 1 shows that how the forty-six questions in the questionnaire are linked with the constructs.

3.5 DATA COLLECTION (DATA GENERATING PROCESS)

For a data generating process three "Ws", who, what and why are of prime importance and these are:

i. Who is missing? Who is counted repeatedly?
ii. What is not measured? And
iii. Why?

There are several methods for data generation, as discussed below

3.5.1 EXPERIMENTS IN LAB

The first one and most common data generating process is Lab Experiments. This method is used in most of the studies normally in which researcher has to work on controlled variables in a systematic way. In these kinds of experiments, researchers have to observe the effect of independent variable say x on one or more dependent variables say y or so on. This type of data generating method can be used in several fields for example in medical field x being the treatment and y being the outcome. These results are applicable on smaller scale and are normally used to check cause of a certain effect for example effect of certain medicine on group of people (test group), works or not i.e. they get cured or remain in same illness.

3.5.1.1 Limitations

1. Data generating via lab experiments is not a suitable process for our kind of research. That's why this type of data generation is not taken into consideration.

3.5.2 FOUND DATA

Another process used for data generation is known as Found Data. This type of data is also called Organic Data as it is largely generated via some ongoing process or uncontrolled data collection method for example Bank Transaction data is regularly collected and saved in database of bank. Similarly, data gathered by CCTVs is collected on regular basis. There are so many other examples. This is an ongoing process and does not answer any research question until or unless a question is designed in such a way that found data helps in answering it in some way.

But there is a big issue in this kind of data as there can be missing pieces of data as all the characteristics of big data are present in it. Which are

1. Volume
2. Velocity
3. Variety and
4. Veracity

3.5.2.1 Limitations

1. As the data set is enormous and doubtful this implies that there must be missing pieces as in CCTVs example there can be some technical fault which cause break in recording. This fact destroys the positive selection probability which is a must have for causal form of research question.

3.5.3 ADMINISTRATIVE DATA

Another data generating process is Administrative data which is generated by governments or industries i.e. production process. For example, tax forms, social security systems, NADRA etc. This kind of data is generated for some cause other than research. This data is generated for administrative and monitoring purposes.

3.5.3.1 Limitations

1. As digitalization process is emerging in all around the world, hence this kind of data is not always in electronic or digital form. Therefore, handling this type of data is not an easy task.
2. Moreover, this type of data is not reliable enough. This is only best for program relevant variables, the mandatory fields marked with asterisk. As people usually do not bother to enter data in fields without asterisk mark therefore, for other fields the quality of data is low. As there must be missing pieces of data which causes non positive selection probability.

3.5.4 SURVEY/ INTERVIEW DATA

The last but not the least and most common data generating process is survey/ interview data. In this method data is collected against a specific research question and the questions are crafted in such a way that must answer the specific research question/objective. The data generated through this method contains variation in both quantity and quality. And this kind of data generation i.e. via surveys is most suitable for this research.

3.5.4.1 Advantages

1. This is suitable process for data generation as it suits to causal type of research questions.
2. Positive and known selection probability is present in this kind of data generation which is must for causal type of research objectives.

3.6 SURVEY

As discussed in previous section that data collection via surveys fits most to this causal research, there exist several modes for surveys [27]. Choosing a data selection mode is a high

impact decision in research design as cost, efficiency or the expected errors that might occur highly depends on data collection method. In surveys there exist different modes for example, Face to Face surveys, Postal surveys, Telephonic surveys, Online surveys and Hybrid or Mix mode surveys. Moreover, the software based surveys and mobile web surveys, text web surveys and video web surveys are the emerging ones. As there are several modes in surveys, each survey has its own specifications in accordance with different dimensions. Brief discussion is as under:

1. In accordance with degree of interviewer involvement there can be three different modes of surveys, these are (a) Interviewer administered, (b) Self-administered in the presence of interviewer, and (c) Completely self-administered.
2. In accordance with the degree of contact with respondents there again can be three categories. (a) Direct contact i.e. face to face surveys, (b) Indirect contact i.e. telephonic, mail or web surveys, and (c) Without contact as in direct observation and administrative records.
3. Considering the channel of communication there can be (a) Aural surveys for example telephonic ones, (b) Visual surveys as mail or web surveys, and (c) the surveys having both aural and visual qualities i.e. face to face surveys with show cards or web surveys on platforms like, zoom or skype etc.
4. Keeping in mind the degree of privacy the three categories are (a) Low privacy: Group administered surveys, intercept surveys and exit surveys, (b) Medium privacy: For example, in home interviewer administered survey, and (c) High privacy: As self-administered survey or computerized questionnaire.
5. In accordance with the involvement of technology, the classification includes (a) without technology: for example, paper based questionnaires and mail based surveys, (b) use of technology by interviewer: for example, computer assisted interviewing, (c) use of survey organization supplied technology by respondent: for example, computer assisted self-interviewing, and (d) use of own technology by respondents: as web surveys.

3.6.1 Approaches of selecting a Mode

Survey mode selection is based on two characteristics:

1. Errors, and
2. Cost

The best survey approach has been considered the one which will be more cost efficient and having less survey errors. Researchers will go for the approach having best tradeoffs between both characteristics.

3.6.2 Survey Mode Selection for this Study

For this research hybrid/ mix mode has been selected [28]. The customized hybrid mode for this research consists of web based online survey using google forms and paper based offline questionnaire-based survey. The reasons behind selection of online survey are as under [29].

1. It is the most cost effective and cheapest survey method.
2. As built-in tools like survey monkey and Google Forms etc. are present. Therefore, online surveys become much easier and user friendly.
3. As due to COVID-19 pandemic situation all over the world, Face to face and contact based surveys became nearly impossible to conduct. Therefore, online survey method has been used as they can be easily carried out amidst lockdown restrictions.
4. Variety of Institutions and cities can be catered via online surveys as we don't have to physically visit any place in this kind of survey.
5. Survey inference becomes more general and accurate.
6. One most important benefit of using online mode for surveys is to get honest answers from respondents as in some cases people do not usually speak the truth in presence of other fellows or interviewers especially about their negative behavior (as will be asked in conduct risk category). Children are also shy about their sufferings and are reluctant to share with others.
7. Along with online survey paper based questionnaires are also used to make a comparison of online and offline survey.
8. Offline survey has been included to check the validity of online survey so that the inference results can be considered more accurate.

3.7 SURVEY LIFE CYCLE

The three aspects of survey life cycle are as under:

1. Survey life cycle from a design perspective
2. Survey life cycle from a process perspective
3. Survey life cycle from a quality perspective

3.7.1 Survey Life Cycle from a Design Perspective

The survey life cycle from a design perspective has two different flow domains. One is Measurement side and the other is Representation side. The blocks on representation side are Construct, Measurement, Response, and Edited Response and finally comes the Survey Statistics. While the representation side contains Population Mean, Sampling Frame, Sample, Respondents, Post Survey Adjusted Data and Lastly the Survey Statistics. Figure 1 shows the flow of survey design process.

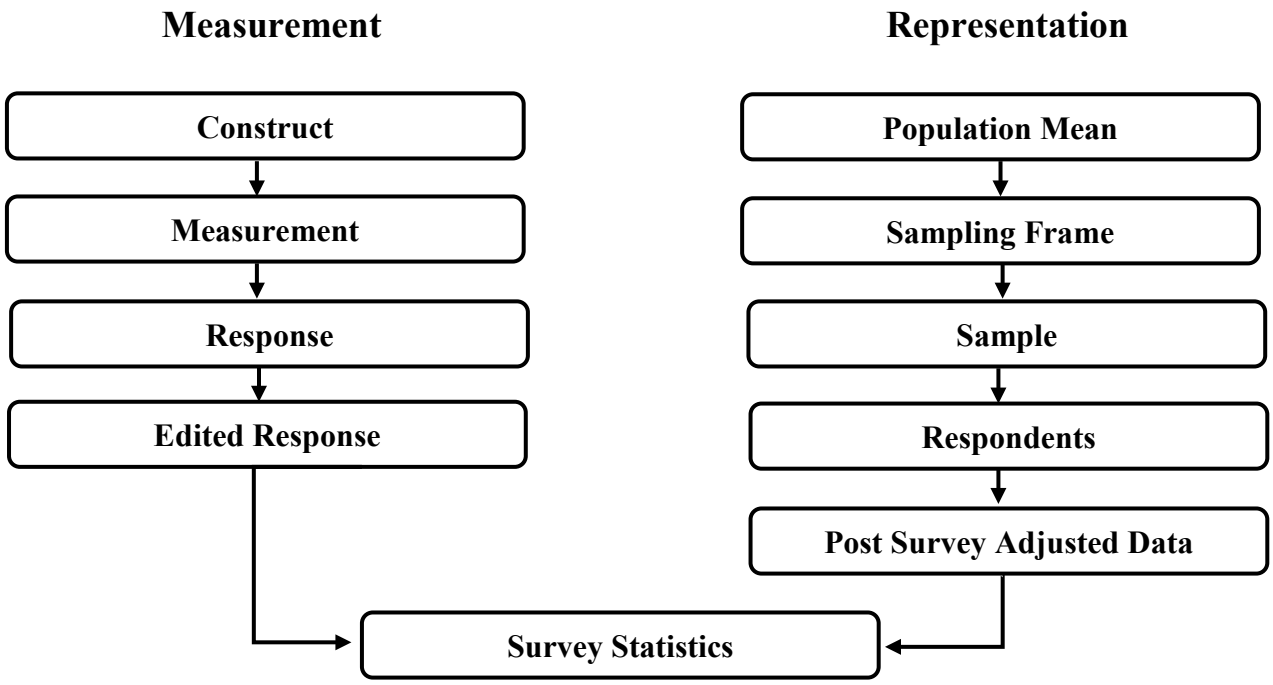


Figure 2: Survey Life Cycle from a Design Perspective

3.7.1.1 Measurement Side

All the four terms of Measurement side of Survey life cycle under design perspective are briefly described as under:

Construct

Construct can be defined as "Elements of Information sought by researcher, usually described by words, often abstract, permitting different more specific definition."

Examples can be "Belief in God", "Quality of life", "Happiness", "Crime".

Measurement

Measurement can be defined as "The method of linking the theoretical constructs to observable variables i.e. Questions, Observations, Blood Pressure readings, Soil samples etc."

For example, for the construct “Crime”, the measurement question will be “Did you call police in last six months to report something that happen to you?” This example shows how the construct “crime” is linked to this question.

Response

Response is the outcome given by the respondent to the measurements.

For example, answers to the questions, quantity of soil, number reading from blood pressure device, record extraction etc.

Edited Response

Value stored in data record used for analysis for specific measure. Resulting from coding text into numbers and acceptable answer sets for example range edits.

3.8 MEASUREMENT SIDE OF SURVEY DESIGN

Measurement side of the survey from design perspective is going to be explained in this section. After thorough research and studying relevant literature, the Internet Risks were categorized in two main categories. One category comprises of those cyber risks which are dependent on human actions or caused by online activities of human beings. The other category contains those internet risks which are usually independent of human actions and are mainly caused by technology. Internet risks categorization is compacted in the form of a flow chart in Figure 2.

3.8.1 HUMAN RISKS

The first category i.e. Human Risks is further divided into three sub categories, which are as under:

3.8.1.1 Content Risks

Those risks that occur due to online available content on different websites and social media platforms that can be unsuitable or inappropriate in some aspects. This can be due to the three types of contents available online.

i. **Provocative Content**: The first one is provocative content that can cause anger or any other type of extreme/ strong reactions, especially deliberately. This kind of content is further categorized into two final constructs which are discussed as under.

   a) **Age-Inappropriate Content** i.e. such type of content that is not suitable for someone’s age e.g. a small child accidently saw an adult 18+ content or drug promotions or some kind of violent content or any other type of content that is not appropriate for his/her age and can have negative influence on his/her mind afterwards. Such type of content engraves

very harsh effects on young minds and haunt them all lifelong. The construct, Age-Inappropriate Content, has been measured by following questions in the questionnaire: *Have you ever seen age inappropriate or adult content online*? (Q-12) and *Have ever seen drug promoting content online?* (Q-13)

b) Second construct under the category of provocative content is more severe and that is **"Content Promoting Bias and Bigotry"**. For example, promoting sectarianism or religious hatred or encouraging regional or provincial bigotry or anti state propaganda on social media platforms by make trending hashtags and promoting biased content. This construct has been measured by questions like *Have you ever seen posts that promote sectarianism and religious hatred?* (Q-14) *Have you ever seen posts that promote provincial bigotry*? (Q-15)

ii. **Incorrect content or false information:** Second type of content risks is the false and incorrect material available online. Construct for this type of content is "Incorrect Content or False Info." And measurement in the questionnaire will be like, *Have you ever seen fake news or false information online?* (Q-16)

iii. **Commercial Content:** The third kind of content risk can harm you personally as well as financially and this is personal commercial content that pop-up on different websites and social media networks in the form of advertisements that usually alter the buyer decision by offering enchanting offers. Commercial content is further classified in two sub categories:

a) **Commercial Exploitation:** includes attractive offers that manipulate the consumer's decision. Some of these advertisements, when clicked accidently, redirects you to websites having unethical and violent content or drug promotions. Children became more fascinated by attractive offers of online game purchase and ring tones purchase. Hence they follow the random instructions given by company's advertisements and results in causing financial loss to their parents. This construct has been measured by following questions in the questionnaire. "*Have you ever altered your decision due to online advertisements?"* (Q-17), "*Have you ever purchased online games or ring tones etc.?"* (Q-18) and, "*Have you ever seen advertisements that lead you to inappropriate content?"* (Q-19)

b) **Unwanted Collection of Personal Data:** Most of the websites and social networking platforms shows enchanting game offers and other attractive advertisements that children usually got attracted to them and click there to get subscriptions. The subscription form then ask for personal information that sometimes include debit card info as well. As usually children use mobile phone devices of their parents, and due to modern AI technologies like autofill option in forms there exist chances of financial losses. This risk lays in a very severe category of online threats as the personal data, like names, DOBs, email addresses, CNICs or Sometimes bank information as well, gathered via these online platforms can be subjected for wrong purposes. There are so many cases in which this kind of data got hacked or illegally breached and is then used for psychological manipulation of minds and even worst purposes (as happened in Cambridge Analytica). This construct is measured by following question in the survey questionnaire: *"Have you ever got a subscription after giving your personal information?"* (Q-20)

3.8.1.2 Contact Risks

Second subcategory of online risks caused by human activities is Contact Risks. This is the most common risk lurking on internet and can cause severe mental disturbances. Contact risks are also further categorized into two sub domains.

i. **Online Risks:** The first one is the online contact risks which is the most serious cyber threat faced by young generation according to Kaspersky research Lab [14]. This badly effects a child's mental health resulting in loss of concentration in his/her daily tasks i.e. studies, playing etc. and the bad thing about this is that children are usually unaware and often do not share about these online sufferings with anyone. Further classification includes following constructs:

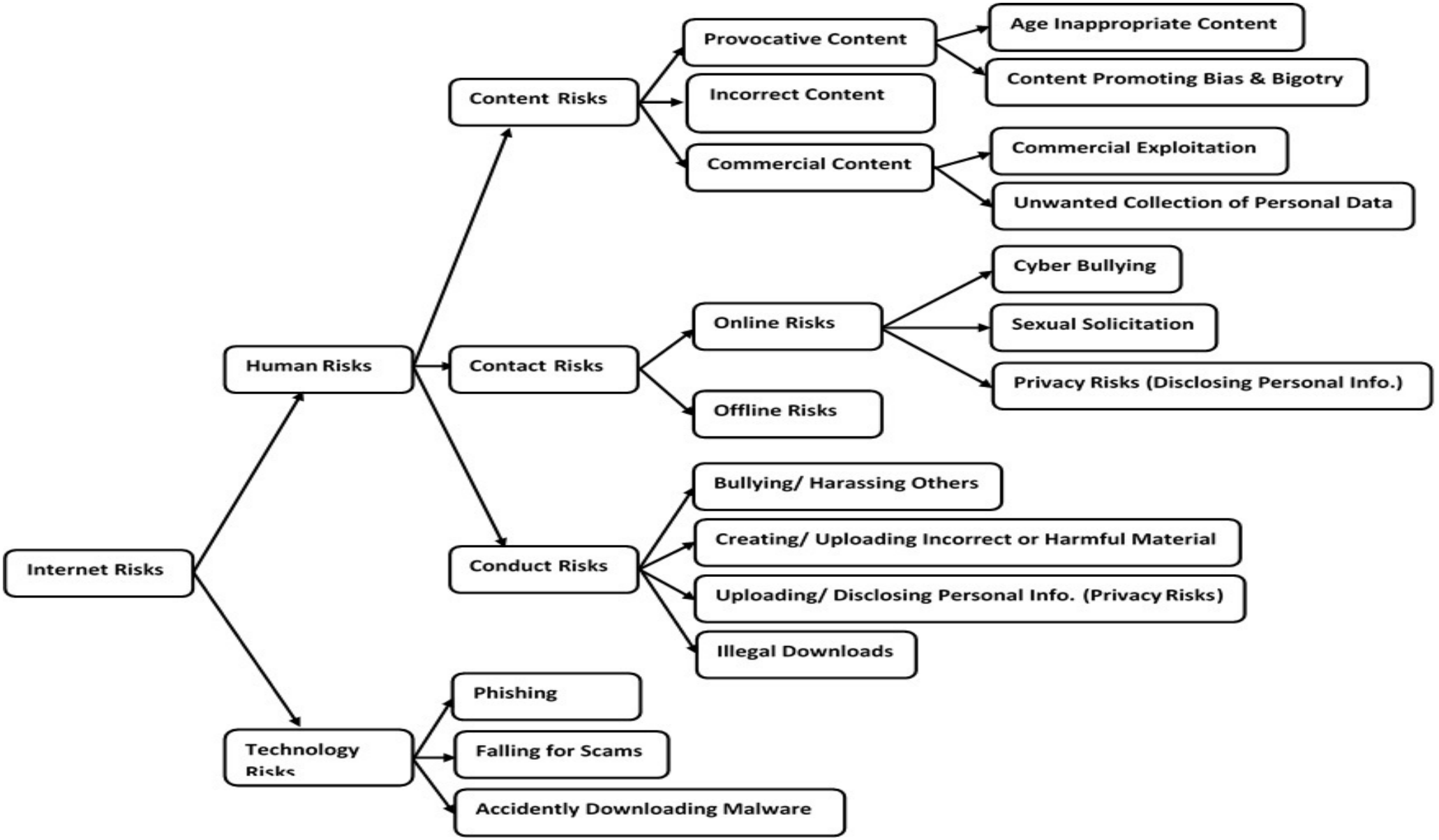


Figure 3: Construct Flow Chart (Internet Risk Categorization)

a) **Cyber Bullying:** The most common cyber risk present on almost all social media platforms and chatrooms etc. is cyber bullying. The measurement for this construct includes questions like *"Have you ever faced abusive or unethical languages on social media and other online platforms?"* (Q-21), *"Have you ever faced humiliation online?"* (Q-22). The predators on social media and other online platforms usually hunt innocent children as their prey. By making fake profiles and hiding their actual identity they initiate contact with online active youth and make them feel trusted on the opponent. After that they assault them by sending vulgar messages and sharing indecent content in texts audios and videos. This type of content is ruinous for a young mind and haunt the young ones afterwards in life and sometimes causes adverse moral damages to them. Measurement for this is: *"Have you ever noticed identity theft or fake profiles online?"* (Q-23)

b) **Sexual Solicitation:** The second and most unethical and adverse cyber risk for social media users and other online community especially for children is sexual solicitation. This is so undesirable/perilous that we cannot directly ask young children and students about it. So the measurement question for this construct is designed in best possible way and is as follows: *"Have someone ever tried to assault you online?"* (Q-24)

c) **Privacy Risks (Disclosing Personal Information):** This construct is also common in online contact risks category. As discussed earlier that children got trapped by predators and develop trust on them, in some cases they even share their passwords with them by hook or by crook. Some kids are so much innocent that they easily share their passwords of their social media profiles and other accounts with their real life or even with their social media friends. This is the riskiest act that a young social media consumer can do. As by making this mistake, all his/her personal data and online profiles became at risk. Measurement for this is: *"Have you ever shared your personal information or data online?"* (Q-25), and *"Have you ever shared your password with someone online?"* (Q-26) Children who consume social media often share their personal life events and celebrations in the form of pictures and

family/friends videos. Sometimes these photos and videos goes viral and create troubles for the families, and sometimes even worst happens, as these pictures /videos goes manipulated by the criminals present out there via editing software and then are used for blackmailing purpose which harms the children, and in some severe cases harms their families as well, mentally, physically and financially. Measurement for this sort of privacy risks is as follows: *"Do you regularly share your daily routine (e.g. family photos and social events) on social media?"* (Q-27) Children sometimes themselves break privacy of others by sharing their personal chats etc. as measured in following question: *"Have you ever read screenshots of personal chats of others?"* (Q-28) The last category in the construct of Privacy Risks is providing access to your online profiles. As there are such kind of games and IQ tests or educational quizzes etc. that ask for access to yours and sometimes to your friend's personal profiles. These entertainment apps, when granted access, collect your personal data for example your interests, DOBs, email addresses etc. that are further used for sending ad-wares etc. Measurement include following question: *"Have you ever filled some sort of psychological or educational quizzes that ask access to yours and your friend's personal data?"* (Q-29)

ii. **Offline Risks:** The second construct category in contact risks is offline risks. All the previously mentioned online risks sometimes get more dangerous and due to unwanted share of personal data i.e. sharing home addresses etc. (privacy risks), the predators sometimes chase children offline physical addresses and then assault them physically which is even more harmful for the child than that of online contact risks. This construct is measured via these questions in the questionnaire: *"Do you have such friends on social media who are unknown to you in real life?"* (Q-30), and *"Have you ever met someone whom you have first met on social media?"* (Q-31)

3.8.1.3 Conduct Risks

The cyber-crimes measured in above two categories of internet risks i.e. Content Risks and Contact Risks, if conducted by a child then emerges this third category of cyber risks i.e. Conduct Risks. Children are so innocent. They usually adopt things from their surroundings

very quickly. If they got interaction with good people online, they learn positivity and vice versa. Due to this some children got addicted to bad online habits and conduct some kind of online faults/crimes that have been discussed in constructs of previous two sections. The construct of this very category and their measurements are as under:

i. **Bullying/Harassing Others:** This construct emerges when the harasser him/herself is a child and is measured by the question: *"Have you ever bullied others online?"* (Q-32)

ii. **Creating/Uploading Incorrect or Harmful Material:** If children themselves share fake information or create/make videos/blogs or posts etc. containing violent content. Children can also be involved in illegal activities like false identity profiles (identity theft). Following questions have been designed for measuring this construct: *"Have you ever shared incorrect or fake information online?"* (Q-33) and *"Have you ever created or uploaded harmful material online?"* (Q-34)

iii. **Privacy Risks (Disclosing Personal Info.):** This construct is about if children disclose someone else's personal information via sharing screen shots of their personal chats or giving access to random access to random apps to their friend's social media profiles etc. The question included in questionnaire for measurement of this construct is: *"Have you ever disclosed others personal data via screenshots etc.?"* (Q-35)

iv. **Illegal Downloads:** There are hundreds and thousands of websites containing pirated versions of books, notes, software and games etc. These websites are insecure and apart from financial fraud, i.e. not giving financial benefit to actual owner/writer/developer by violating copy rights, these websites are also a big source of spreading malwares. The measurement for this construct is: *"Have you ever downloaded pirated version of games or books etc.?"* (Q-36)

3.8.2 TECHNOLOGICAL RISKS

The second broad category is Technological risks, which comprises of those internet risks which are not directly dependent on human action in usual and are mainly caused by technology. Further categorization into constructs is as under;

3.8.2.1 Falling for Scams

Scammers exist in a vast variety and in a big number in the virtual world. They allure netizens by offering attractive offers as free download of games etc. There are such

algorithms that are designed for showing children such offers, considering their age and then redirect them to illegal pages having many of above mentioned internet risks. The measurement for this construct is: *"Have you ever seen such offers as free access to online games etc.?"* (Q-37)

3.8.2.2 Accidently Downloading a Malware

As scam offers, insecure websites and adware often redirects the user to malicious pages that are main cause of malware downloading. Children usually get in trouble due to this. The measurement for this construct includes following questions; *"Have you ever clicked on a link that automatically downloads a malware/virus that troubles you later on?"* (Q-38), *"Have you ever download a game that shows a lot of advertisements?"* (Q-39), and *"Have you ever downloaded a game that causes data corruption or virus etc.?"* (Q-40)

3.8.2.3 Phishing

Phishing is a kind of attack under social engineering category. In this, the victim receives emails or messages from legitimate persons (family/ friends etc.) but are not actually sent by them. These are forged email/messages as identity theft have been occurred in them. By opening such kind of fraudulent emails/messages, the user's data (often including login credentials and credit card information etc.) are stolen. Measurement for this construct category includes questions like: *"Have you ever got such emails that ask you to click on links that redirects you to malicious pages?"* (Q-41), *"Have you ever received such SMSs as mentioned in previous question?"* (Q-42), and *"Have you ever got an email from a legitimate family member or friend that was not actually sent by them?"* (Q-43)

The last two questions of the questionnaire are of miscellaneous nature. And measure the reaction of a child after facing any of above mentioned online risks, i.e. *"What was the impact of all above situations on your mind?"* (Q-44) and *"Have you ever informed anyone (Parents/Siblings/Teachers) for proper guidance?"* (Q-45)

Table 3-1: Measurement Table

CONSTRUCT	SUB CATEGORY	MEASUREMENT
Basic Internet Usage		Q No. 1, 2, 3, 4, 5, 6,7
Basic Awareness Level		Q No. 8, 9, 10,11
Content Risks	Age Inappropriate Content	Q No. 12, 13, 14
	Content Promoting Bias and Bigotry	Q No. 15, 16
	Incorrect Content	Q No. 17
	Commercial Exploitation	Q No. 18, 19, 20
	Unwanted Collection of Personal Data	Q No. 21
Contact Risks	Cyber Bullying	Q No. 22, 23, 24
	Sexual Solicitation	Q No. 25
	Uploading Personal Information	Q No. 26, 27, 28, 29, 30
	Offline Contact Risks	Q No. 31, 32
Conduct Risks	Bullying/ Harassing Others	Q No. 33
	Creating/ Uploading False/ Harmful Material	Q No. 34, 35
	Privacy Risks (Disclosing Personal Info.)	Q No. 36
	Illegal Downloads	Q No. 37
Technological Risks	Falling for Scams	Q No. 38
	Accidently Downloading Malware	Q No. 39, 40, 41
	Phishing	Q No. 42, 44
Miscellaneous Questions		Q No. 45, 46

3.8.3 Basic Internet Usage

Similarly, the initial six questions of the questionnaire measure basic internet usage routine of the children. As the life has become totally changed after the COVID-19 pandemic for all the individuals. Same occurred with the children. Especially due to online education, their focus diverts from entertainment to other meaningful purposes of digital world. To measure this the first two question of the questionnaire has been designed as *"What was your favorite online activity before COVID-19?"* (Q-1) *"What is your favorite online activity after COVID-19?"* (Q-2) Next comes the questions measuring internet access and usage details. *"Do you have access to any computer, mobile or tablet with internet facility?"* (Q-3) *"Have you ever used webcam?"* (Q-4) *"How much time (in hours) you spend on internet daily?"* (Q-5) *"Do you have any access to internet other than home and school computers?"* (Q-6) *"Do you have access to social media accounts?"* (Q-7) *"Do you have your own (personal) social media accounts?"* (Q-8).

3.8.4 Basic Awareness Level

The next four questions are aimed to measure the basic awareness level of students about cyber risks lurking out there in virtual world. These are: *"Have you activated security settings on your social media accounts?"* (Q-9) *"Are you aware of harms/ threats of unsafe internet usage?"* (Q-10) *"Do you know once you posted something online can never be erased?"* (Q-11) *"Have someone (parents or teachers) ever briefed you about online safety?"* (Q-12)

The questions in the questionnaire belongs to which construct is listed in Table 1.

As the above discussion is about measurement side of design perspective of our Survey/Questionnaire Life Cycle. The constructs and their measurements have been discussed in detail. Now comes the representation side of our survey design perspective.

3.9 REPRESENTATION SIDE OF OUR SURVEY DESIGN

The terms in this side of Survey life cycle from design perspective as shown in Figure 1 are described below:

3.9.1 Target Population

This term means the set of units to be studied in the survey. This set is often abstractly defined to have several ways to operate set. For example as in this study has aimed to explore the level of cyber security awareness in young children of Pakistan.

3.9.2 Sampling Frame

Sampling frame refers to the identified set of unit that should be sampled and located. In an ideal sampling frame every unit of the target population appears only once and nothing else would be included in the sampling frame. For example all young generation using social media and online learning platforms and school and college going children are the sampling frame in our case.

3.9.3 Sample

Sample is the subset of sampling frame population that has been chosen for measurement in the survey. For example in this study for online survey the young Pakistanis using different social media platforms and school online groups are the sample. And for the offline survey students of public sector institution in Islamabad are considered as sample.

3.9.4 Respondents

Respondents are the sample units that are successfully contacted and measured.

3.9.5 Post Survey Adjustments

Post survey adjustments are the changes that are made in record collected via survey data set to remove Total Survey Errors (TSE) so that the survey estimates that are made on the basis of this data set better reflect the entire targeted population. We will be discussing this in detail in next chapter in which survey results will be deliberated.

3.10 SURVEY LIFE CYCLE WITH PROCESS PERSPECTIVE

Survey life cycle with respect to the processes involved in survey is shown in Figure 3. These processes are briefly explained as under.

3.10.1 Research Objective

Our research objective is to Gauge Level of Cyber Security Awareness in Young School/College going Pakistani Children and to improvise it.

3.10.2 Sampling Frame

Our sampling frame includes all young generation of Pakistan (school and college going children) using social media and online learning platforms or using internet for any mean.

3.10.3 Design and Select Sample

Designing of sample for online survey is random, the young Pakistanis using different social media platforms and school online groups are the sampling frame and are contacted via online study groups and friends and family. And for the offline survey students of public sector

institution in Islamabad are considered as sample and FTF interviewer administered paper questionnaire are used for this purpose.

3.10.4 Mode of Collection

We have chosen hybrid mode of data collection i.e. both online and offline survey approaches are used.

3.10.5 Construct and Pretest Questionnaire

Constructs are build according to online risk categorization as shown in Figure 2. And the measurement questions are designed accordingly as have been discussed in detail in section 1.8. The designed Questionnaire is then initially pretested on children in family and friends circle to get the feedback about understandability of the questionnaire and to seek the loop holes to overcome the shortcomings.

3.10.6 Modifications

Following are the few modifications that are made after pretesting the questionnaire:

1. Many of the terminologies of online threats were not much familiar to the children. Hence, there meanings in Urdu language have been included in the questionnaire in order to increase the level of children understanding.
2. Some questions are rephrased to make them simpler. A few more questions are added to clearly elaborate the designed constructs.
3. Some of the technical terms used for threats present in cyber world are elaborated in question wording.

3.10.7 Measuring Sample

The measuring process has been done by creating Questionnaire via Google Forms for online survey and a paper based offline face to face survey has also been for measuring the sample.

3.10.8 Code and Edit Data

For coding and editing of data Microsoft excel has been used as it is still considered as one of the most power full tools of data analysis.

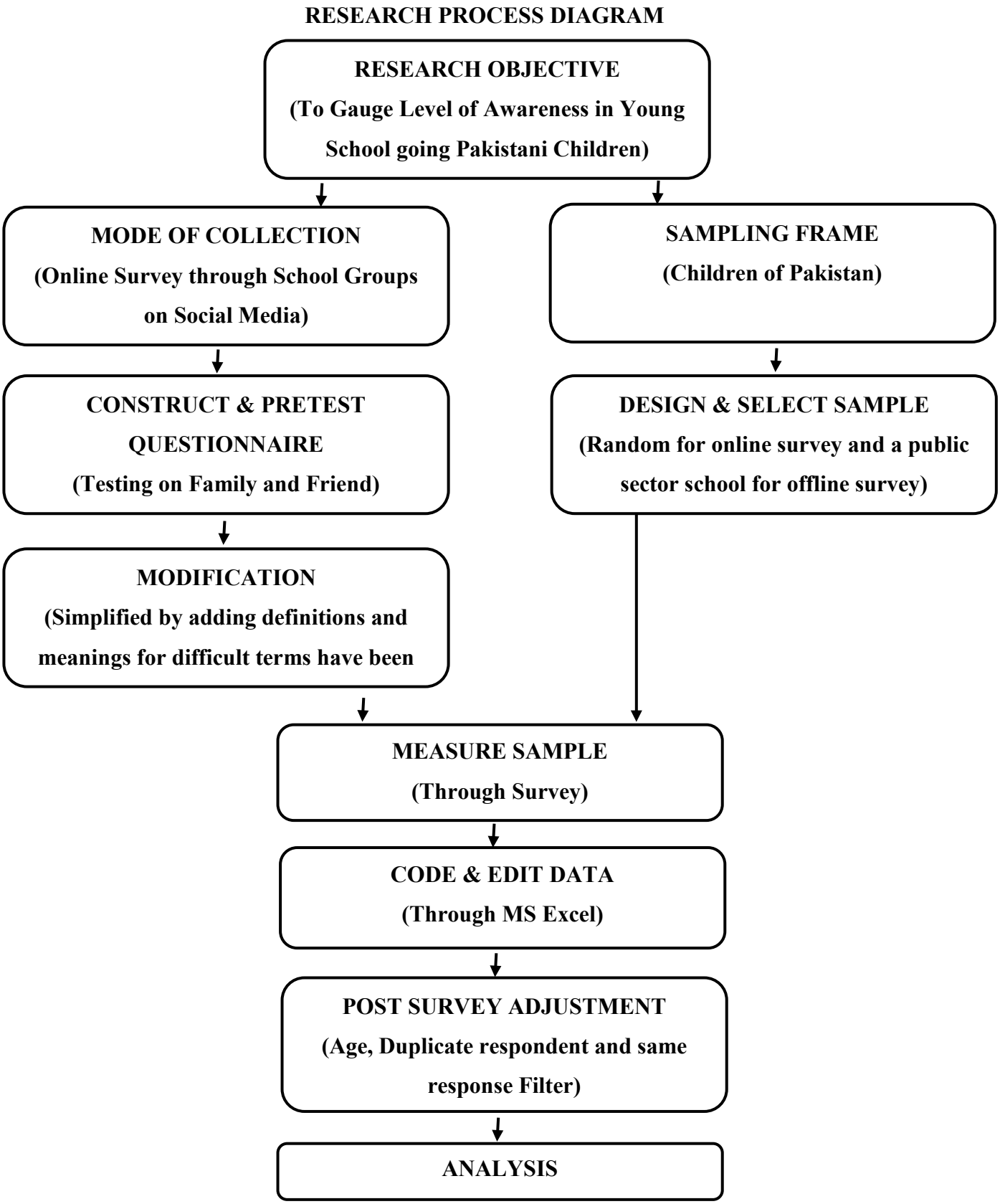


Figure 4: Survey Life Cycle with Process Perspective

3.10.9 Post Survey Adjustments:

The data collected via both surveys has been adjusted and cleaned up. The respondents who gave responses multiple times has been deleted. Similarly, the respondents of age more than 18 years of age are also filtered out as the research scope is to explore cyber security in children of Pakistan and Word children is used for the individuals less than 18 years of age.

3.10.10 Analysis:

The analysis techniques will be discussed in detail in the chapter including results and findings.

Chapter 4: QUESTIONNAIRE DESIGN

4.1 Questionnaire DESIGN

In general, attitude questions are very popular in surveys that are defined as "Those questions that are not verifiable by external record or observation or any other external mean. It is personal experience of each and every individual." There exist three kind of Questions that are usually measured via surveys. These are:

1. ***Attitude (Evaluation Component):*** The questions measuring attitude of a person for example "Have someone ever briefed you about online safety?"
2. ***Belief (Cognitive Component):*** The question that measure your existing thought about some matter, usually without any proof for example "How safe is the internet?"
3. ***Behavioral Intentions (Behavioral Component):*** These are the questions aimed to measure behavioral intentions of the respondents. For example, "Will you tell anyone if you ever faced any of internet threats?"

Most of the questions in this research's questionnaire belongs to the first category to achieve the requirement of measuring attitude of the children towards online safety.

4.2 DIFFERENT VIEWS ABOUT ATTITUDES

4.2.1 Traditional views about Attitudes

According to Cacioppo and Petty [30], "An attitude is an enduring positive or negative feeling about some person object or issue." In views of Eagly and Chaiken, "A psychological tendency that is expressed by evaluating a particular entity with some degree of favour or disfavour."

The above two classical definitions of attitude shows that attitudes contain following characteristics:

1. Attitudes are pre-existing
2. These are retrievable and are automatically activated
3. Attitudes are stable i.e. these are independent of both context and time
4. Attitudes are predictive of behavior
5. And lastly, attitudes are resistant to persuasion

4.2.1.1 Objections

If traditional view is considered for this study, then there is no need to measure the attitude as it is pre-set in mind and goes generation after generation.

4.2.2 Alternative View

According to Zaller, “Indiviualls do not typically possess true ‘attitudes…’ rather, they construct ‘opinion statements’ on the fly … based on whatever considerations are momentarily salient.” As he rephrased this concept as “Making it up as you go along” And in Schwarz view “Construal models conceptualize attitudes as evaluation judgments, formed on the spot, rather than as trait-like disposition.” In short, Attitudes are constantly changing.

4.2.2.1 Objections

1. If we consider the alternative view as true, then measuring attitudes is no more beneficial as the Attitudes are constantly changing.
2. It means people don’t possess stable summary evaluations stored in memory. If some attitude question is asked people construct them on the fly.
3. Top of the head responses based on whatever happens to cross a person’s mind.
4. You will get a different answer for the same question, by the same respondent on the next day.
5. By a small change in the wording of question’s statement or the question’s order, you will get a completely different respond.
6. As according to this view, people construct responses on the fly, this implies that they will report “attitudes” about things that do not even exist.

4.2.3 Resolving the Divergent Views

Researchers tried to resolve the objections came up on the previously discussed two views in his own way by clarifying the difference between Attitude and Attitude Expressions [27]. In author’s opinion “Attitude is unobservable, global evaluation of the objects”. Whereas The Attitude expression is “The specific response to a specific question asked at a particular time in a particular way.” Hence, any single attitude-measure will be an imperfect reflection of the underlying attitude. In conclusion, Attitude expressions may be divided into three categories:

7. Some attitude expressions are entirely constructed on the spot as in Zaller’s view.
8. Other attitude expressions are almost completely retrieved from the memory.
9. Most of the attitude questions are constructed, but the chief ingredient in this construction is the fairly stable overall summary evaluation retrieved from the memory.

4.3 IMPORTANT CONSIDERATIONS FOR QUESTIONNAIRE DESIGN

For a questionnaire design some implications must be kept in mind. Some of them are context related for example, questionnaire wording, sequence of questions, and presentation of the questionnaire, characteristics and behavior of the questionnaire, survey's introduction and external factors such as mood or weather. The other issues include specific or global evaluations, Agree/Disagree scales, hypothetical questions and filtering out the respondents that do not know much about the topic.

4.3.1 Context Effect

The influence of context on the survey is evident from research. Context will influence the response when it affects what enters into consideration while comprehending a question or making a judgement. Hence it is important to consider the context effect with all aspects in a questionnaire design. There are several aspects of the context effect as subject of the questionnaire, interview setting, interviewer's behavior, instructions given in the questions, pictures that accommodate a question to enhance/elaborate it, wording of a question, the given response options and the question order. Broadly, these can be divided into two categories of the context.

1. The first one is Comprehension effect which is further categorized in two sub domains having strong implications on questionnaire design:
    i. Assimilation Effect: It means the respondent keep including prior questions in interpreting the current one.
    ii. Contrast Effect: It is opposite to the previous one i.e. the respondent exclude the prior questions while answering the current item.
2. The second category is Retrieval. At this stage context prompts the accessibility. For example if the question is asked about a scandalized politician first, trustworthiness ratio in response will decrease. If generally asked about trustworthiness of politician without mentioning any special person, than response rate will be quite high.

4.3.2 Specific vs General Evaluation

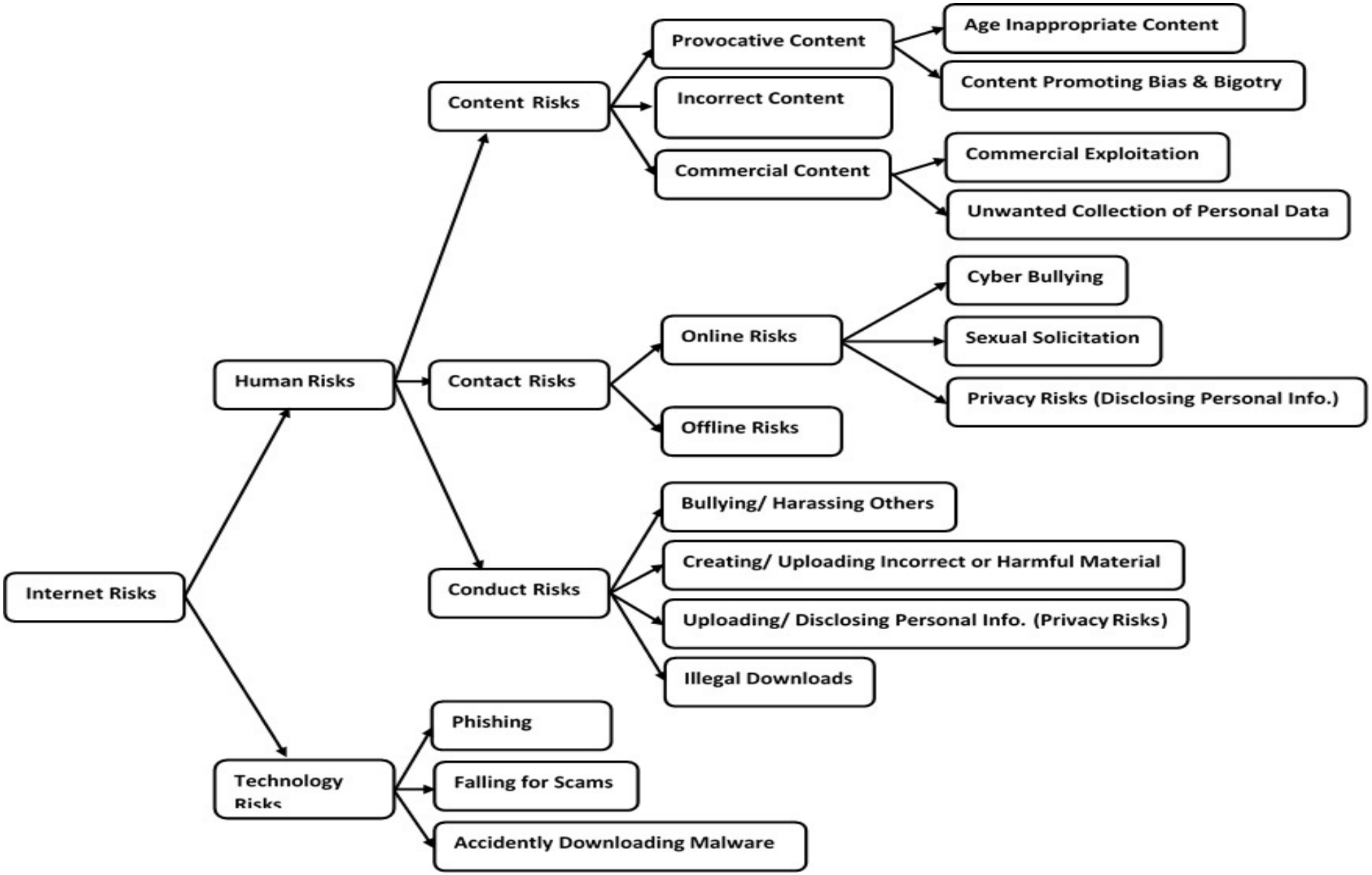
If it is compulsory to ask as specific question at first, then use subtraction effect to erase the influence of previous context from the respondents mind. For example, ask the question like that: "Apart from that specific politician (name), how trustworthy the politicians are?"

4.4 QUESTIONNAIRE DESIGN FOR THIS STUDY

By taking into consideration all the factors discussed in previous sections, research questionnaire has been designed in a systematic way i.e. Questions are aimed to measure the attitude of respondents towards online safety and awareness about internet threats. Secondly context effects has also been kept in mind as the general questions about internet accessibility and usage are asked first (Q-1 to Q-10) followed by questions relevant to specific constructs designed according to Internet Risk Categorization (Q-11 to Q-45). These questions sequence and categorization has been discussed in detail in Measurement section. The detailed discussion has been done in previous chapter that was about Research Methodology. Although the Construct flow chart Figure 1 and measurement table 1 are given here for reference. The main Questionnaire is attached in Appendix A.

Table 4-1: Measurement Table

CONSTRUCT	SUB CATEGORY	MEASUREMENT
Basic Internet Usage		Q No. 1, 2, 3, 4, 5, 6,7
Basic Awareness Level		Q No. 8, 9, 10, 11
Content Risks	Age Inappropriate Content	Q No. 12, 13, 14
	Content Promoting Bias and Bigotry	Q No. 15, 16
	Incorrect Content	Q No. 17
	Commercial Exploitation	Q No. 18, 19, 20
	Unwanted Collection of Personal Data	Q No. 21
Contact Risks	Cyber Bullying	Q No. 22, 23, 24
	Sexual Solicitation	Q No. 25
	Uploading Personal Information	Q No. 26, 27, 28, 29,30
	Offline Contact Risks	Q No. 31, 32
Conduct Risks	Bullying/ Harassing Others	Q No. 33
	Creating/ Uploading False/ Harmful Material	Q No. 34, 35
	Privacy Risks (Disclosing Personal Info.)	Q No. 36
	Illegal Downloads	Q No. 37
Technological Risks	Falling for Scams	Q No. 38
	Accidently Downloading Malware	Q No. 39, 40, 41
	Phishing	Q No. 42, 43, 44
Miscellaneous Questions		Q No. 45, 46


Internet Risks
Human Risks
Technology Risks
Content Risks
Contact Risks
Conduct Risks
Provocative Content
Incorrect Content
Commercial Content
Age Inappropriate Content
Content Promoting Bias & Bigotry
Commercial Exploitation
Unwanted Collection of Personal Data
Online Risks
Offline Risks
Cyber Bullying
Sexual Solicitation
Privacy Risks (Disclosing Personal Info.)
Bullying/ Harassing Others
Creating/ Uploading Incorrect or Harmful Material
Uploading/ Disclosing Personal Info. (Privacy Risks)
Illegal Downloads
Phishing
Falling for Scams
Accidently Downloading Malware

4.4.1 Scaling Techniques

Many researches on scaling techniques show that in survey response options Agree and Disagree Scales are the most common ones. This scaling techniques has its own advantages and disadvantages which are discussed below.

4.4.1.1 Advantages

Advantages of this format are as under:

1. Ease of Administration
2. Response rate is about two third faster in this format as compared to other formats.
3. This format contains fewer Don't Knows as compared to Yes/No scale. Don't know option is not recommended by the researchers as it is dealt as missing pieces in the data.
4. Respondents mostly prefer this format as it is more familiar and common.

4.4.1.2 Disadvantages

Disadvantages in Agree/Disagree scale are the following:

1. Usually respondents want to appear more polite and opt agree scale which destroys the reliability of results.

4.4.2 Recommended Response Options

Construct specific response choices are recommended to choose. As these are more specific and relevant to the subject that is to be measured.

4.4.3 Response Options in Research Questionnaire

For this study, it has been decided to design construct specific response options and five response options format has been selected for maximum of the questions. As for the Question 1 and Question 2 regarding favorite online activity before and after COVID-19 respectively, the respondents have been given five choices that includes the most common online activities for the children, i.e. Entertainment (Movies, Cartoons, and Songs etc.), Social Media, Online Gaming, Online Study and Online Shopping. They have also been given the option of any other and are asked to specify that activity that is not included in the list. Respondents must grade them from 1 to 6 on the basis of their involvement in these activities. Then come the questions relevant to basic Internet Usage from Question 2 to Question 6. As these questions ask about internet and mobile devices accessibility so the given response options are just Yes and No except Question 3 which asks about time specification in hours that they spend on internet. Response options for this question are: Up to 3 hours, 3 to 6 hours, 6 to 9 hours, 9 to 12 hours and more than 12 hours.

Next four questions, Question 7 to Question 10 are to gauge basic awareness level of the children about cyber risks. The response options given for these again include Yes/No options. Next comes the actual core of the questionnaire. The questions that are aimed to measure the internet risk categorization described in previous section. As recommended in research, construct has been to specific response choices. For these questions, i.e. from Question 11 to Question 45 the response options are: All of the time, Most of the time, Some of the time, A little of the time and Never. Except Question 30 and 31 which ask about offline meetings with online friends. These two questions contain different set of response choices which are Yes, all of them, Yes, Many of them, Yes, Some of them, Yes, A few of them and No. And the second last measurement question of the questionnaire which asks about the negative impact of internet risks on young minds have list of top online risks as asset of responses these are Bullying, Harassment, Violent/Adult Content, Religious hatred/Provincial bigotry, Fake news, Disclosure of personal data (pictures etc.) and accidently downloading a virus.

Chapter 5: RESULTS AND DISCUSSION

5.1 INTRODUCTION

To explore the level of Cyber Security Awareness in Young Children of Pakistan we have conducted two surveys. The first one was self-administered computer based online survey. And the second one was Interviewer administered paper based survey. This chapter focuses on the results and findings that we have achieved on the basis of analyzing the survey results after post survey adjustments and removing the survey errors in the best possible way. For this purpose, Survey Life Cycle from a Quality Perspective have been analyzed.

5.2 SURVEY LIFE CYCLE FROM A QUALITY PERSPECTIVE

Quality of a survey depends upon minimizing the error at all steps of the survey. Another thing that must be kept in mind is that errors are not always the mistakes. Some errors just represent the uncertainty that cannot be avoided especially sampling errors that occur during sampling. To reduce the errors and enhance the quality of survey the Total Survey Error (TSE) approach has been followed.

5.2.1 Total Survey Error (TSE)

Total Survey Error is the way of thinking about different sources of errors that may affect the statistical data gathered via surveys. A [31] s the goal of the survey is to make the inference to a broader population, for this purpose it is necessary to mitigate the errors to improve the quality of survey. Survey quality is the measure of the success of inferential goal.

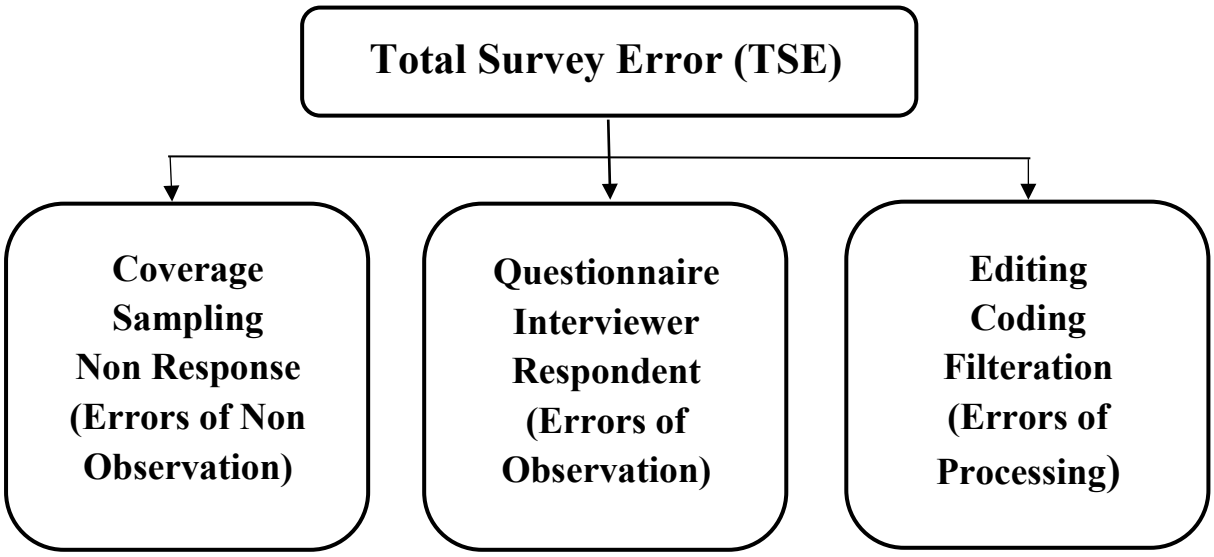


Figure 6: Total Survey Error (TSE)

5.2.1.1 Measurement Errors

1. This occur when the designed question doesn't exactly measure the concept. To avoid this kind of error a thorough study has been done on the internet risks and categorization has been done in four main domains and further sub domains that are termed as constructs of the survey and measurement questions have been designed accordingly.
2. If the question exactly measures the construct, the chances of errors still exists if the respondent may face difficulty in understanding the question or recalling the relevant information. To overcome this issue the questions have been designed in the simplest language as possible and also added meanings of difficult terms in Urdu language as intended audience are the children.
3. This kind of error may also occur if the interviewer is asking about some sensitive information or socially undesirable behavior, same is the case with the questionnaire of this study especially with the conduct risk category. The main reason behind selecting of web based self-administered questionnaire was to avoid this kind of measurement error. As for collecting honest responds from the respondent, web based questionnaires are more assumed to be near the truth. However in the Face to Face paper based survey the possibility of this kind of error is still present.

5.2.1.2 Representation Errors

Coverage Error:

Coverage error refers to the population that is not under coverage due to certain reasons. For example as in our case in online survey the people who are not using internet cannot be measured and in offline survey. This unavailability can be due to several reasons such as (a) less income, (b) less education, (c) lack of interest, (d) residence in non-signal zone i.e. rural areas etc. This unavailability is a very serious concern in online surveys but not in this case as the study aimed to measure online threats in young children of Pakistan and those who are not available online are already out of our target population. Secondly, in offline survey as we have targeted a public sector institution so our target population is already limited.

Sampling Error:

Drawing a smaller sample from the target population that doesn't perfectly represent the target population is referred as sampling error. In web based survey this is not necessary as No sampling is one of the approach in online surveys. And for offline survey not every institution is contactable.

Non response Error:

This kind of error includes refusal to contribute and non-contactable and is the main source of error. That cannot be mitigated.

5.3 PARA DATA

From online Survey, responses have been received from one hundred and twenty one respondents from twenty five different cities countrywide. The responses came from Rawalpindi, Karachi, Lahore, Quetta, Islamabad, Sargodha, Khushab, Hadali, Jauharabad, Faisalabad, Rawalakot, Lawa, Hyderabad, Gujjar Khan, Bagh, Mian Channo, Okara, Peshawar, Attock, Talagang, Bhakkar Bar, Chakwal, Pelowance, Joyia, and Multan. The respondents are between 10 to 41 years of age and are students of different schools, colleges, and universities all our the country, and belong to various fields of studies from primary and middle school levels to PhD students of various technical and non-technical fields as Pre-Medical, Pre-Engineering, ICS, IT, Commerce, Arts and Humanities, Information Security, Mathematics, Mass Communication, Fashion Designing, Accounts, Computer Sciences, Medical, Zoology, Software Engineering, Banking and Finance, Urdu and Economics. The collected Responses have repeated ones and out of age bound responses as the targeted population was Children of Pakistan under 18 years of age. And from the offline survey we gathered data from eighty five respondents from public sector institution of Islamabad Federal Area from middle and secondary classes. The gathered data was raw data and need a lot of post survey adjustments. Are you having some spare time these days?

5.4 FILTERING AND CLEANING UP THE DATA

After gathering the data from the survey and organizing it in spread sheets the next step done was of cleaning up the data. Cleaning up means getting rid of the scores that are meaning less either because of some outliers that can't be true or may be because of somebody went through the survey very quickly and gave the same answers for every measurement in the questionnaire. These kind of responses are not data. These are just noise that's why getting rid from that is important to get meaningful data and to meet the inferential goals.

5.4.1 Cleaning up Online Survey Data

The data gathered via online survey was cleaned up from noise in the following two ways:

1. As the respondents vary from primary to PhD students, there ages vary between 10 years to 41 years. Target population in this research are Pakistani children and according to research the term children is applied to the individuals under 18 year of age therefore, 31

respondents who were not matching the age bound and are from 19 to 41 years of ages had been filtered out.

2. Secondly some of the respondents filled the questionnaire twice with same answers every time, these kind of responses had also been considered as noise and deleted to get clean authentic data.

After cleaning of the data had been done, the actual number of respondents reduced to nighty one from one hundred and twenty one. Thirty of the responses were treated as noise.

5.4.2 Cleaning up Offline Survey Data

Cleaning of Offline data had been done on the following base:

1. Some of the respondents just checked the same option for all the questions. This shows the lack of interest in the survey and considered as noise. And hence been deleted.
2. Some of the respondents marked 'Never' or 'No' option for all measurement questions. This clearly showed that these respondents are not much familiar with internet and are out of the scope of the research hence deleted.

Initially data from eighty five respondents was taken and after filtering out the noise remaining respondents were fifty eight. Data from twenty six respondents was filtered.

5.5 RESULTS AND FINDINGS OF ONLINE SURVEY

After scaling and filtering the raw data into meaning full data, the tabulation and graphing process have been done. The data have been categorized into subsets according to the designed constructs as discussed in the previous chapter. Following are the details of gathered data.

5.5.1 BASIC INTERNET USAGE

Table 5-1: Data of basic Internet Usage

Questions	Construct	TOTAL	BLANK ANSWERS	YES (%)	NO (%)	TOTAL (%)
Question 2	Internet facility	**91**	0	90%	10%	**100%**
Question 3	Webcam	**90**	1	34%	66%	**100%**
Question 5	Internet outside Homes & Schools	**91**	0	38%	62%	**100%**
Question 6	Access to Social Media	**90**	1	83%	17%	**100%**
Question 7	Personal Social Media Accounts	**91**	0	69%	31%	**100%**

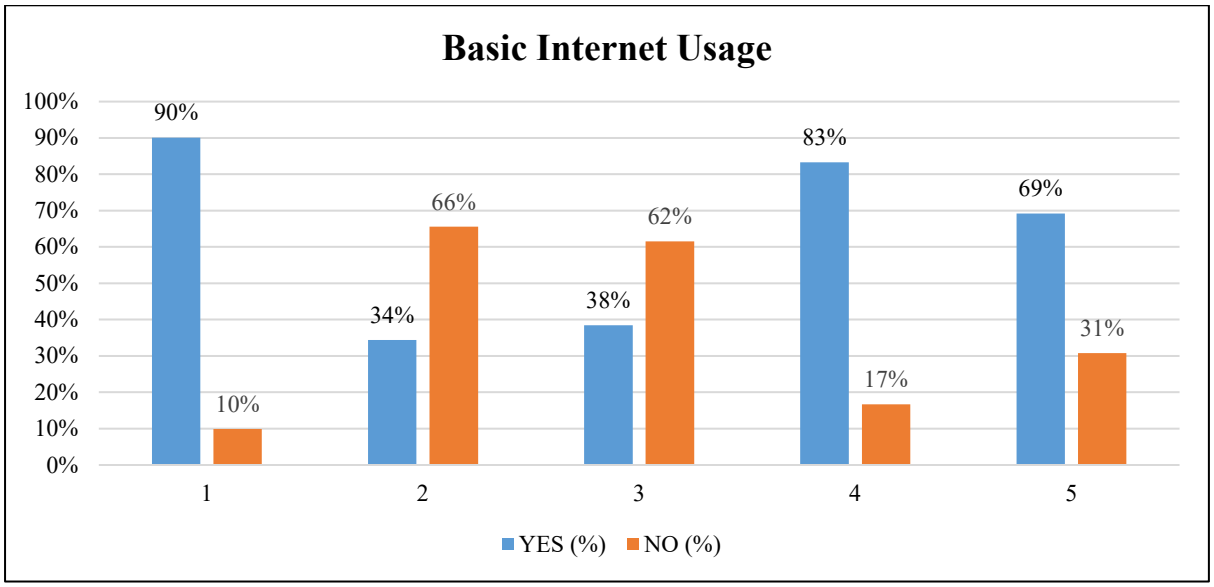


Figure 7: Basic Internet Usage

The first Categorization after initial introduction questions in the designed questionnaire was about to measure basic internet usage of the target population. How familiar are they with the internet devices and how many have access to the online platforms. Results shows that 34 % children are using Webcam, 90% of them had internet facility and 38% have this facility outside school and homes as well. As for social media usage 83% of them has access to social media accounts of their own or parents or siblings while when asked about their own social media accounts than this percentage reduced from 83% to 69%. Next table shows the percentage in hours of how much time children spend on internet daily.

Table 5-2: Time Spent on Internet (in hours)

Internet Usage	No of Responses	Percentages
Up to 3 hours (%)	44	**48%**
3 to 6 hours (%)	20	**22%**
6 to 9 hours (%)	14	**15%**
9 to 12 hours (%)	5	**5%**
More than 12 hours (%)	8	**9%**
TOTAL (%)	91	**100%**

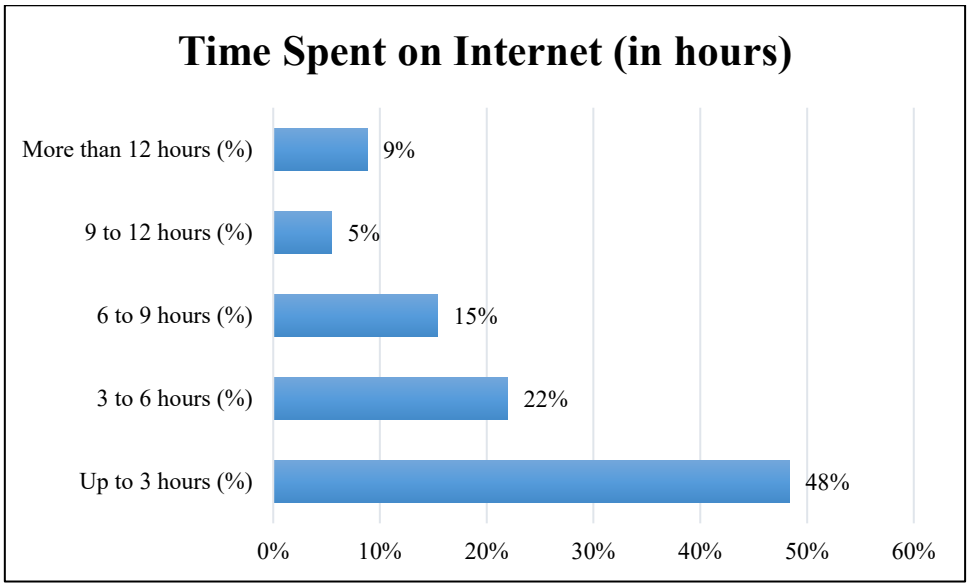


Figure 8: Time spent on internet

The statistics shows that about half of the population of targeted sample i.e. 48% spend limited time on internet that is up to 3 hours per day, and half of the remaining half i.e. 22% spend up to 6 hours daily online while the remaining population although less in number but their internet usage time increases. 15% of them spend more than quarter of a day online i.e. up to 9 hours, 5% spent almost 12 hours it means half of a day and online. And there are 9% severe cases who spent more than half of their day on internet.

5.5.2 BASIC LEVEL OF AWARENESS:

The next categorization includes questions about basic level of internet risks awareness. The gathered data is tabulated as under.

Table 5-3: Basic level of Cyber Security Awareness

Questions	Construct	TOTAL	BLANK ANSWERS	YES (%)	NO (%)	TOTAL (%)
Question 8	Activated Security Settings	**91**	0	69%	31%	**100%**
Question 9	Aware of Unsafe Internet Usage	**90**	1	79%	21%	**100%**
Question 10	Online stuff is Inerasable	**90**	1	49%	51%	**100%**
Question 11	Briefing about Online Safety	**90**	1	67%	33%	**100%**

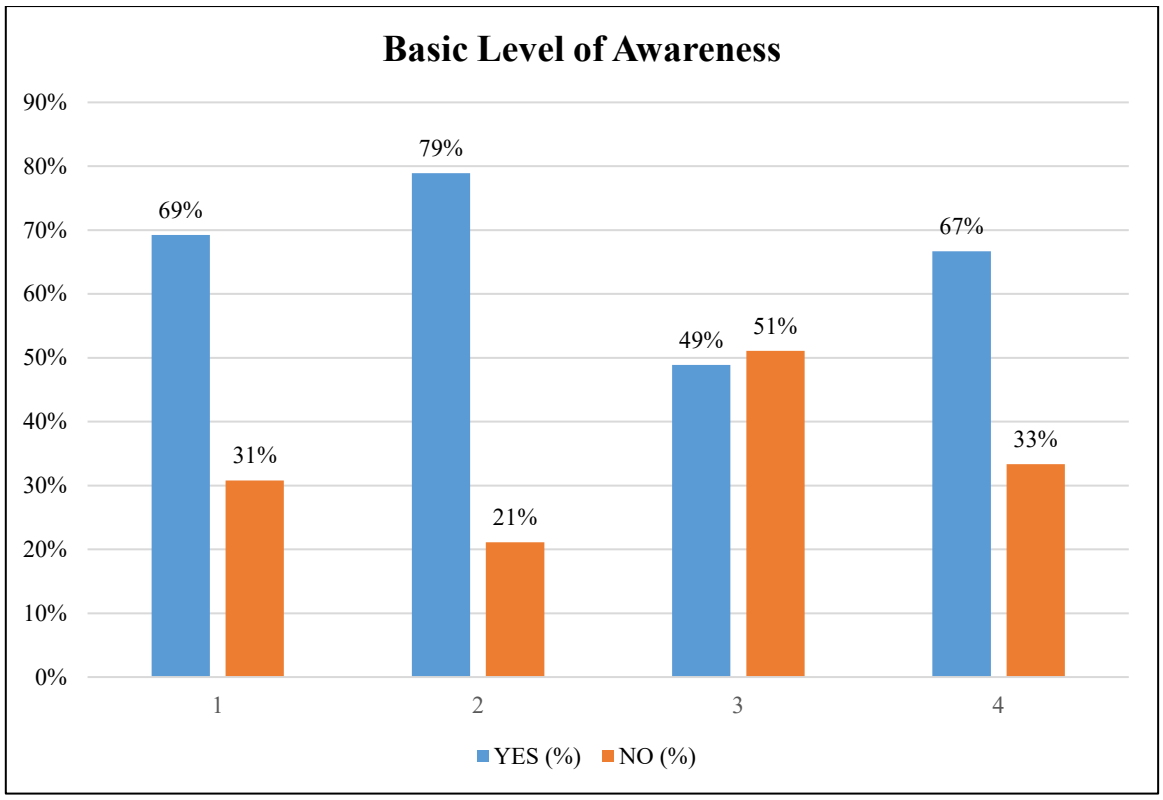


Figure 9: Basic Awareness Level

The responses shows that 69% of children in targeted sample have activated security settings provided by the social media developers, 79% told that they are familiar with harms and threats of unsafe internet usage, but only 49%, less than half, knows that the material once posted online can never be erased, and 67% were briefed by their parents or teachers about internet risks.

5.5.3 Content Risks

Internet Risk Categorization starts from here. Initially internet risks are divided into four categories. The first one is Content Risks. This category is further divided into sub domains namely Provocative Content, Incorrect Content and Commercial Content. Further categorization makes the construct which are measured in the questionnaire and results and findings are discussed below accordingly.

5.5.3.1 Age Inappropriate Content

Age inappropriate risk is the first construct from this category. The age inappropriate content can be, adult content, violent content or drug promoting content. Following is the data of three questions related to this construct.

Table 5-4: Data of Age Inappropriate Content

Age Inappropriate Content								
Questions	**TOTAL**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 11	**91**	0	2%	7%	16%	23%	52%	**100%**
Question 12	**88**	3	0%	9%	24%	28%	39%	**100%**
Question 13	**91**	0	0%	3%	13%	19%	65%	**100%**

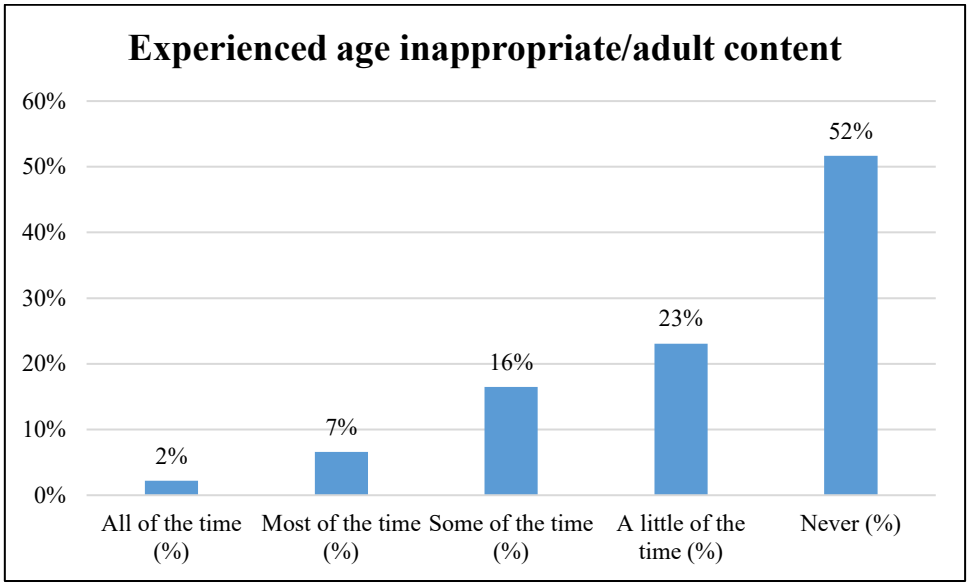


Figure 10: Experienced age inappropriate content

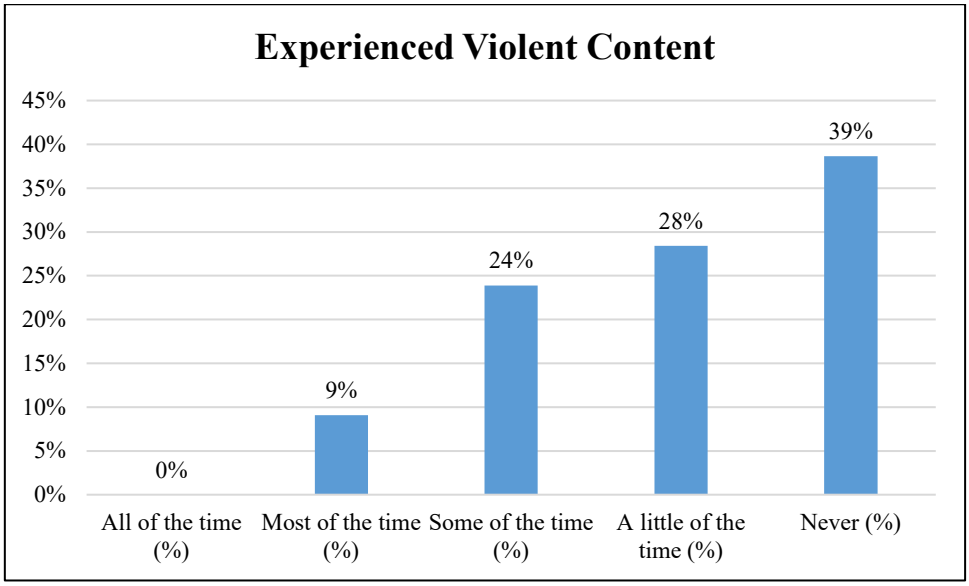


Figure 11: Experiences Violent Content

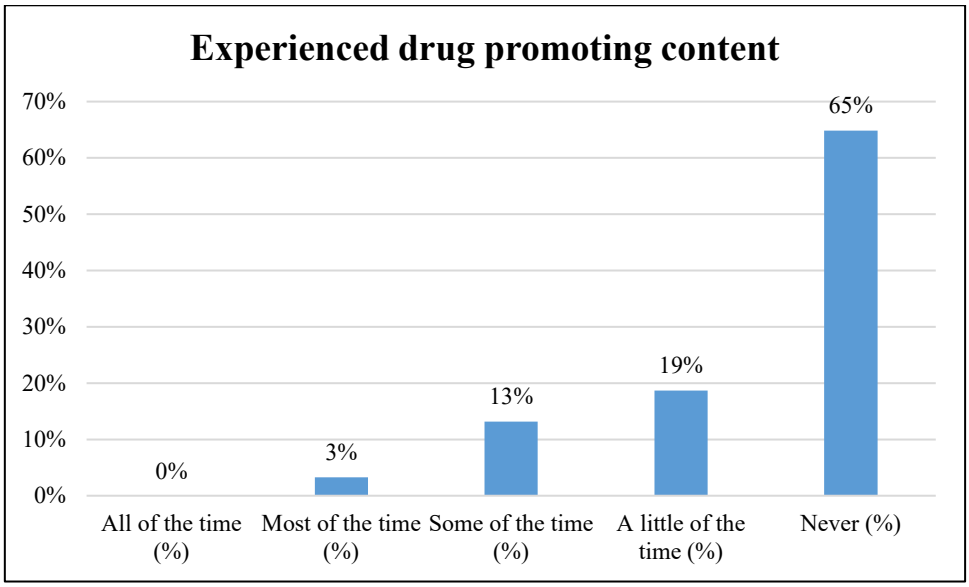


Figure 12: Experienced drug promoting content

Above figures show the data of children who have experienced the three kinds of age inappropriate content i.e. adult, violent or drug promoting content in which frequency. Most of the children replied as 'Never' but still there is a large number who have experienced this kind of unwanted content. Violent content is the most experienced from all the three types of Age inappropriate content.

5.5.3.2 Content Promoting Bias and Bigotry

Two questions were included in the questionnaire to measure content promoting bias and bigotry. The results are tabulated below.

Table 5-5: Content Promoting Bias and Bigotry

Content Promoting Bias and Bigotry								
Questions	**TOTAL**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 15	90	1	4%	14%	19%	14%	48%	100%
Question 16	88	3	6%	10%	10%	25%	49%	100%

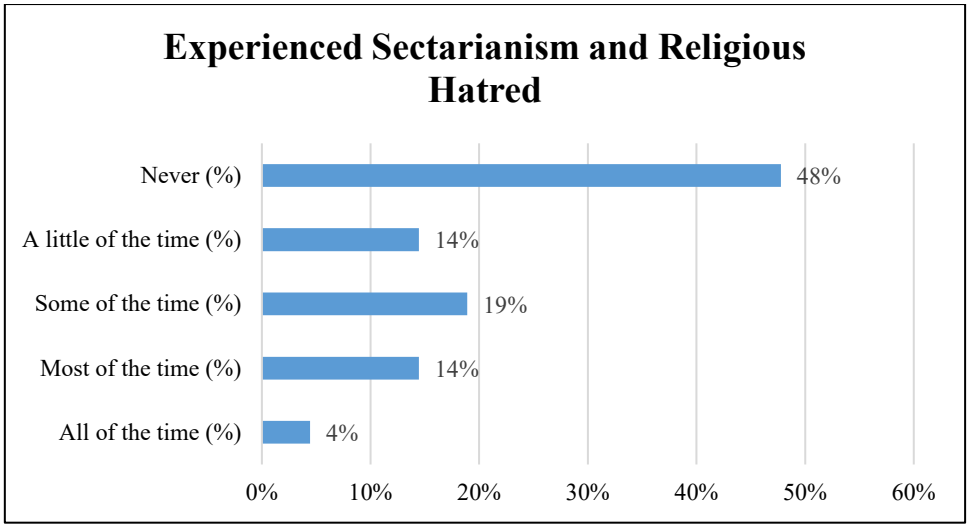


Figure 13: Experienced Sectarianism

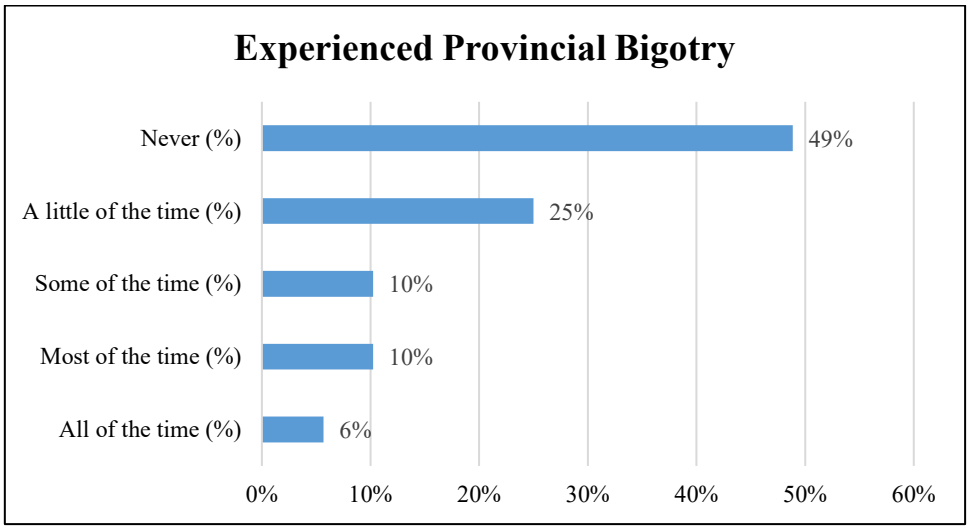


Figure 14: Experienced Provincial Bigotry

The first question about this construct was related to sectarianism and religious hatred and the second one was intended to measure provincial and linguistic bigotry. More than half, i.e. 52% and 51% of the children in the target population has seen posts related to sectarianism and provincial bigotry respectively.

5.5.3.3 Incorrect Content

False information and Fake news are one of the most common content risk available online. And the results shows that the internet risk from which children are affected the most is Fake news. According to survey 90% of the targeted sample population of the children has experienced this internet risk.

Table 5-6: Fake or Incorrect Information

Fake News or False Information								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 17	90	1	19%	39%	21%	11%	10%	100%

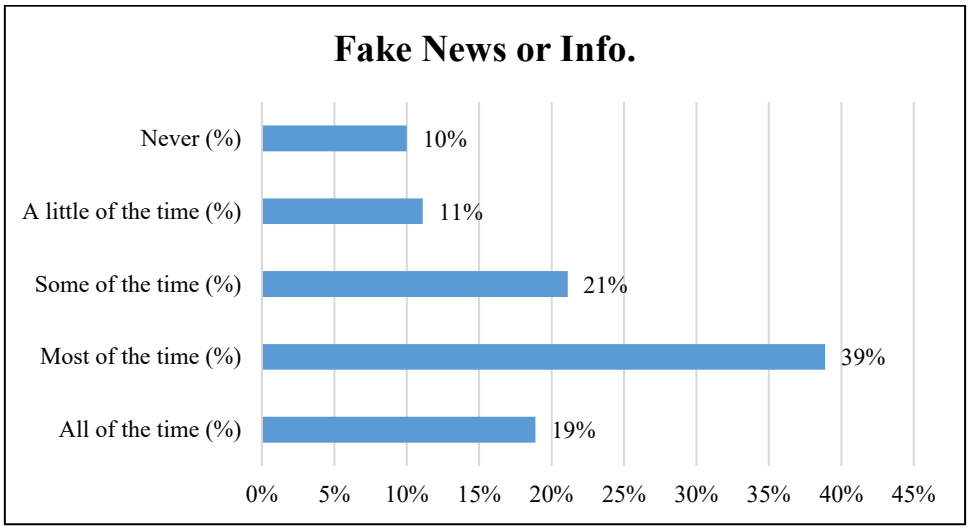


Figure 15: Experienced Fake News

The Results shows high suffering of the children from False and Incorrect information that become viral on internet without authentication and reference. As in current pandemic situation fake notifications about opening and closure of schools became viral.

5.5.3.4 Commercial Exploitation

Commercial content is also one of the most occurring content risk on social media platforms and other web sites. Three questions have been included to measure its occurring intensity and the results are tabulated as under:

Table 5-7: Commercial Content

Commercial Exploitation								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 18	90	1	0%	4%	20%	28%	48%	100%
Question 19	89	2	1%	2%	10%	11%	75%	100%
Question 20	88	3	1%	7%	19%	27%	45%	100%

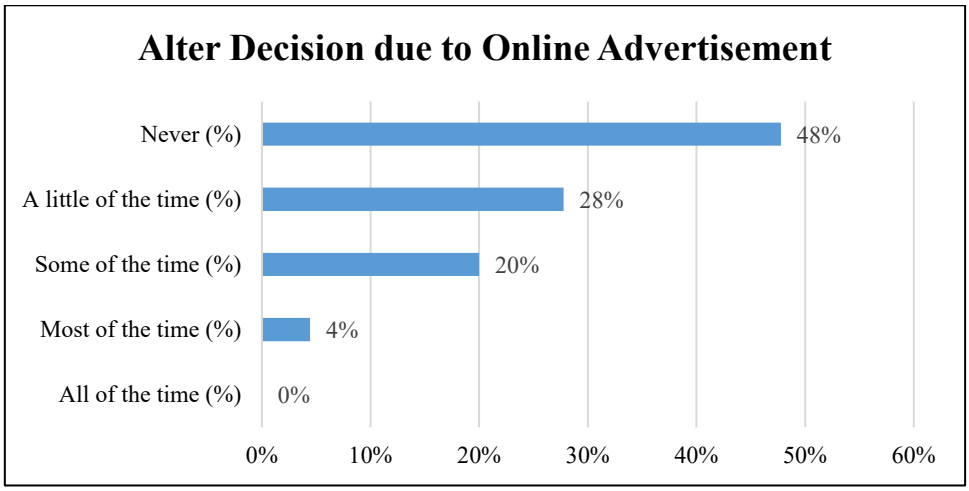


Figure 16: Decision change due to online Advertisements

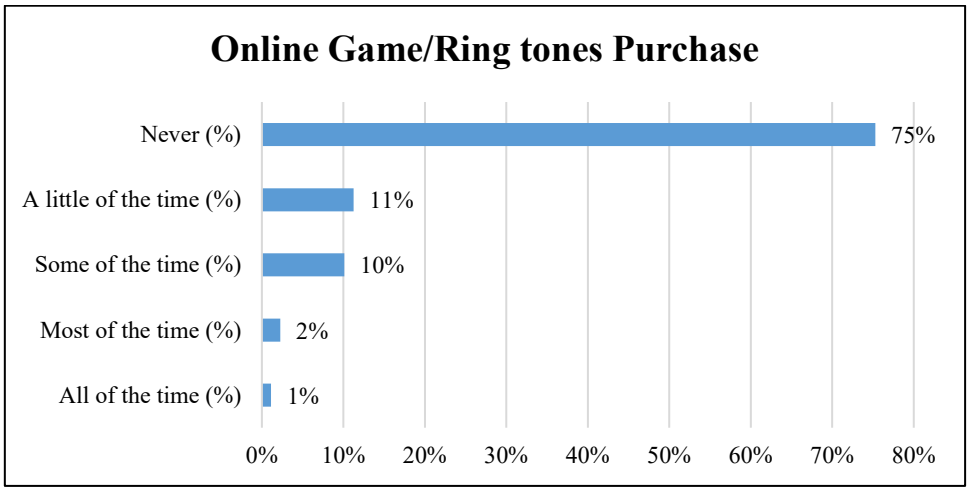


Figure 17: Online Games/ Ring Tones Purchase

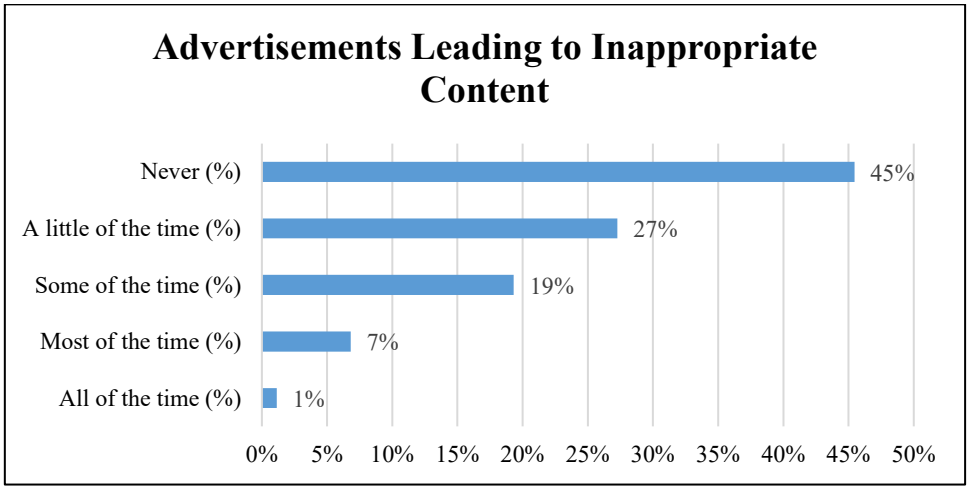


Figure 18: Advertisements Leading to Inappropriate Content

52% of the children have altered their decision due to online advertisements, percentage of purchasing of online games or ringtones is quite low but still 25% of children still gone through this. And the highest risk category in this domain is in which advertisements lead to inappropriate content. 55% of the targeted sample has faced this risk in different frequencies as shown in the graph.

5.5.3.5 Unwanted Collection of Personal Data

The last sub domain of content risk is unwanted collection of personal data. In this domain children are asked for giving their personal data for subscription of games or home-work websites etc. This was measured by one question and the results show that more than half i.e. 51% of targeted children have got such subscriptions.

Table 5-8: Unwanted Collection of Data

Unwanted Collection of Personal Data								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 21	88	3	5%	10%	14%	23%	49%	100%

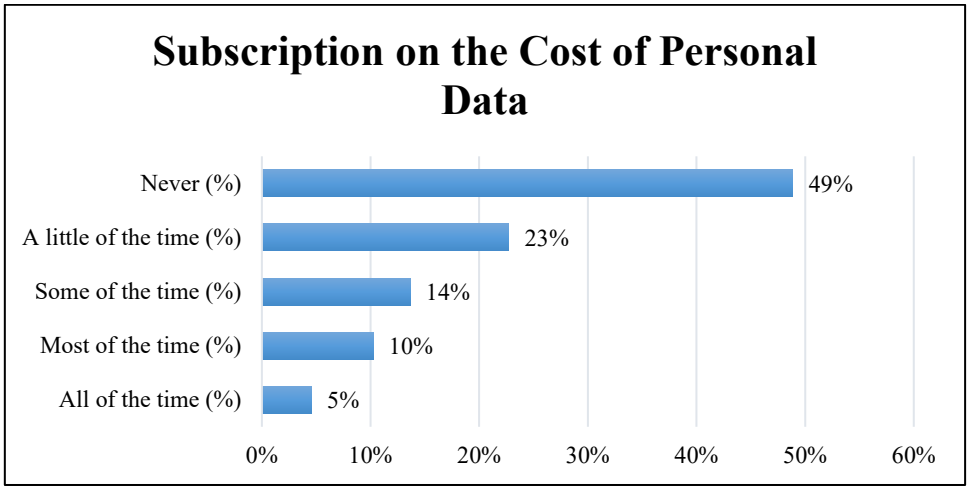


Figure 19: Unwanted Collection of Data

5.5.4 Contact Risks

Second domain of Human Risks is Contact risks.

5.5.4.1 Cyber Bullying

It is the first and most common sub category of Contact Risks domain. The result of three measurement questions is as under:

Table 5-9: Cyber Bullying

Cyber Bullying								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 22	88	3	3%	7%	24%	17%	49%	100%
Question 23	89	2	1%	0%	11%	31%	56%	100%
Question 24	89	2	6%	30%	19%	17%	28%	100%

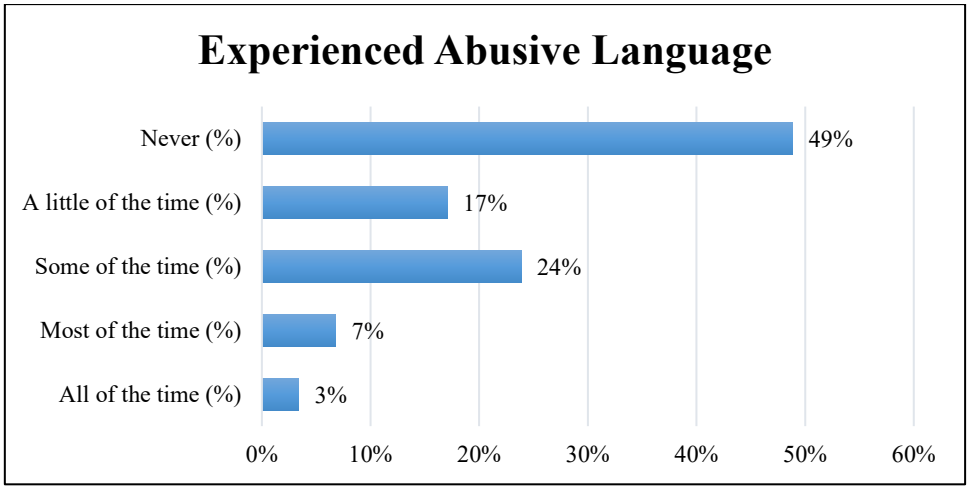


Figure 20: Faced Abusive Language

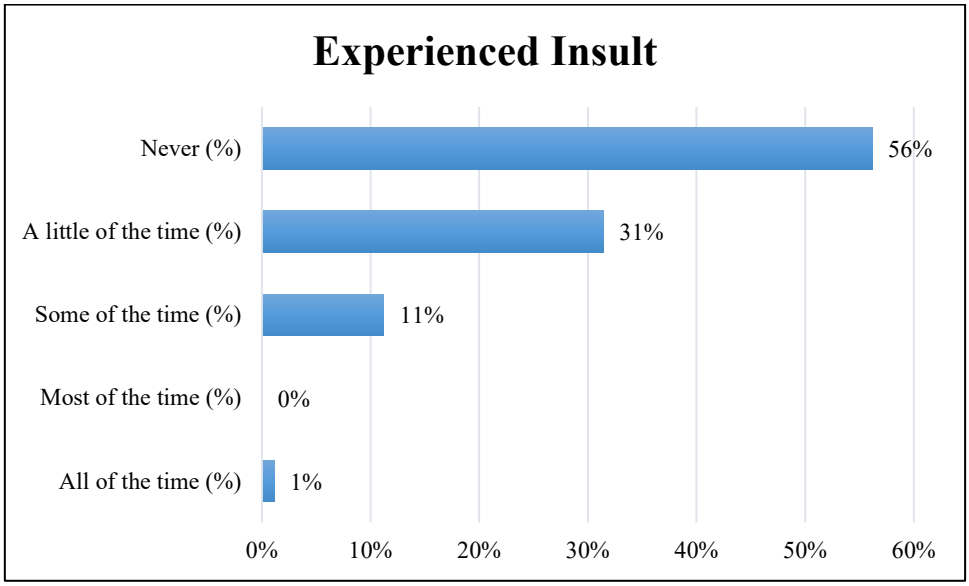


Figure 21: Felt Humiliation Online

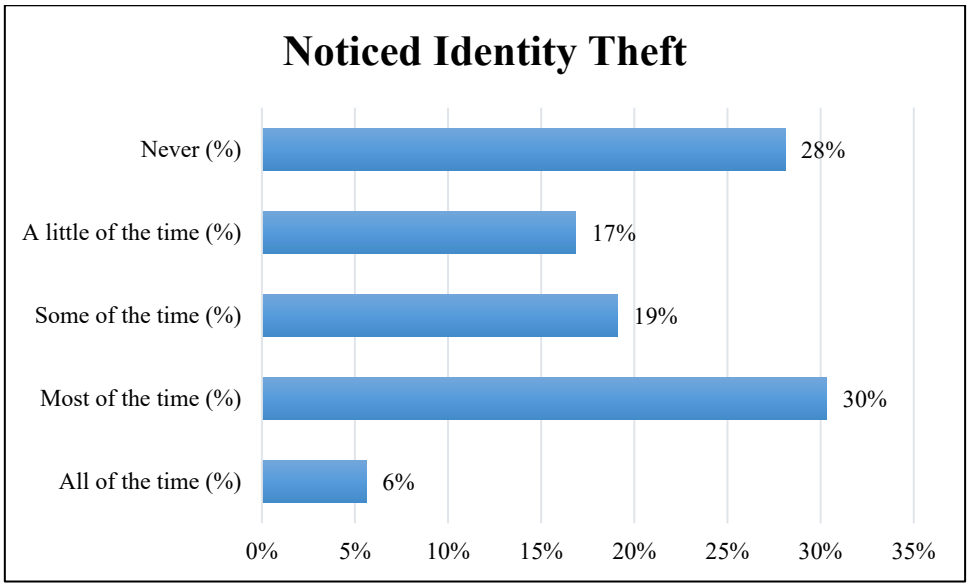


Figure 22: Noticed Fake Profiles

51% of children have faced abusive language, 44% of them has felt humiliated due online negative behaviors of other and 72% of them have noticed identity theft and fake profiles which is a large number.

5.5.5 Sexual Solicitation

The most unethical and unwanted contact risk is sexual exploitation. And 25% of the students reported to experienced online harassment.

Table 5-10: Online Harassment

Online Harassment								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 25	89	2	0%	4%	10%	10%	75%	100%

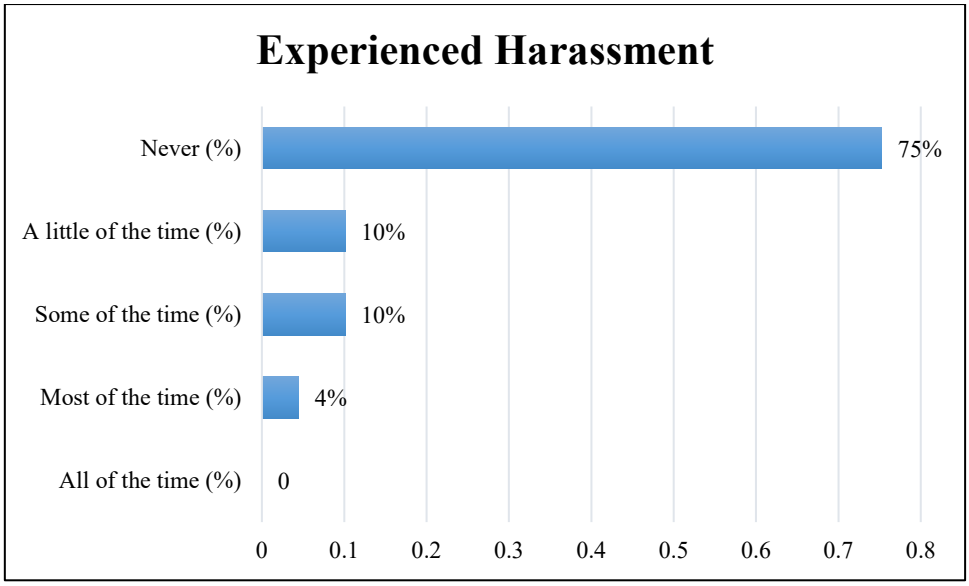


Figure 23: Experienced Harassment

5.5.5.1 Uploading Personal Information

This is the broadest category of contact risks. The questionnaire included five questions to measure all the aspects. Results are tabulated below.

Table 5-11: Uploading Personal Information

Uploading Personal Information online								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 26	89	2	8%	3%	9%	21%	58%	100%
Question 27	89	2	0%	3%	3%	8%	85%	100%
Question 28	89	2	3%	2%	13%	25%	56%	100%
Question 29	89	2	3%	8%	17%	27%	45%	100%
Question 30	88	3	2%	5%	14%	14%	66%	100%

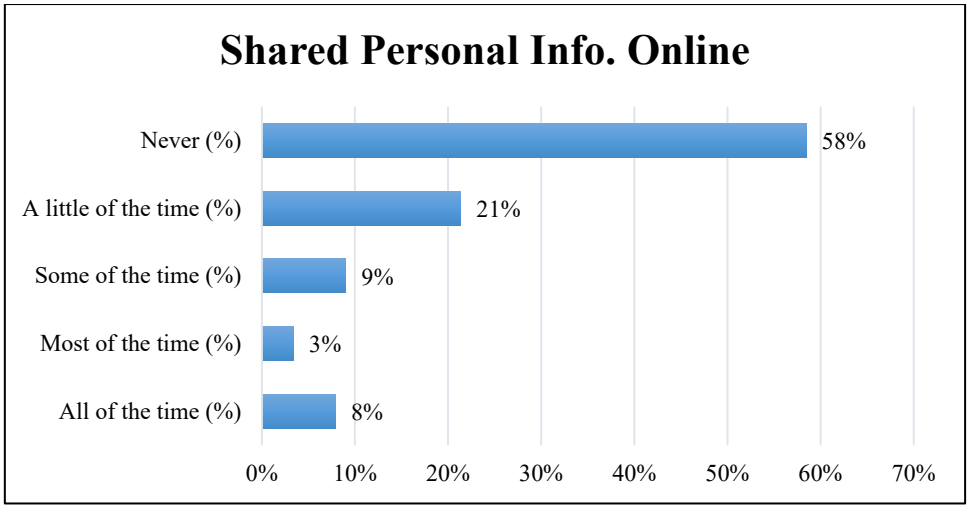


Figure 24: Shared Personal Information

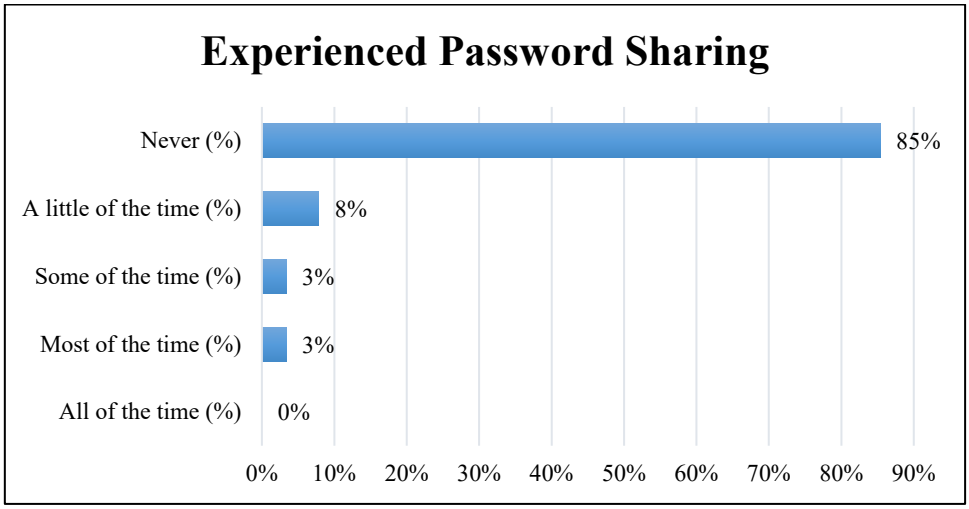


Figure 25: Shared Password with Someone

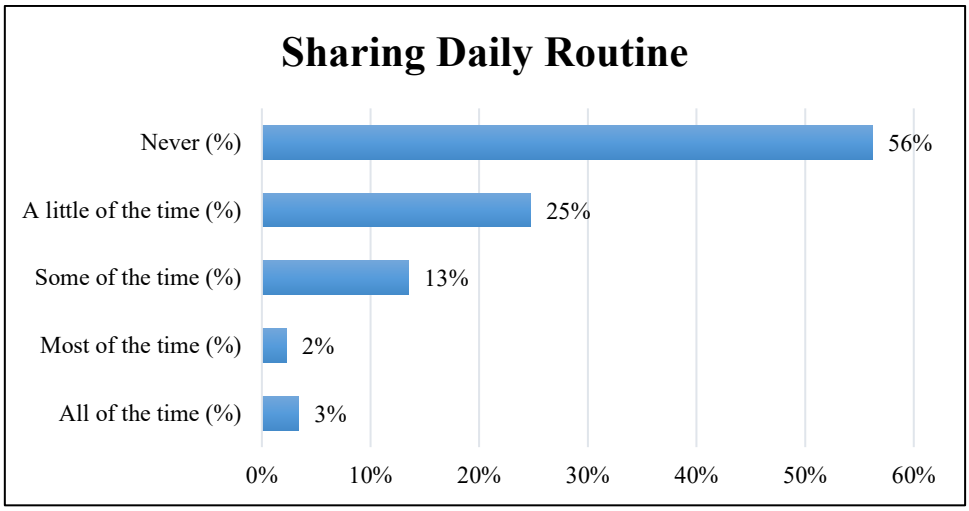


Figure 26: Shared Daily Routine

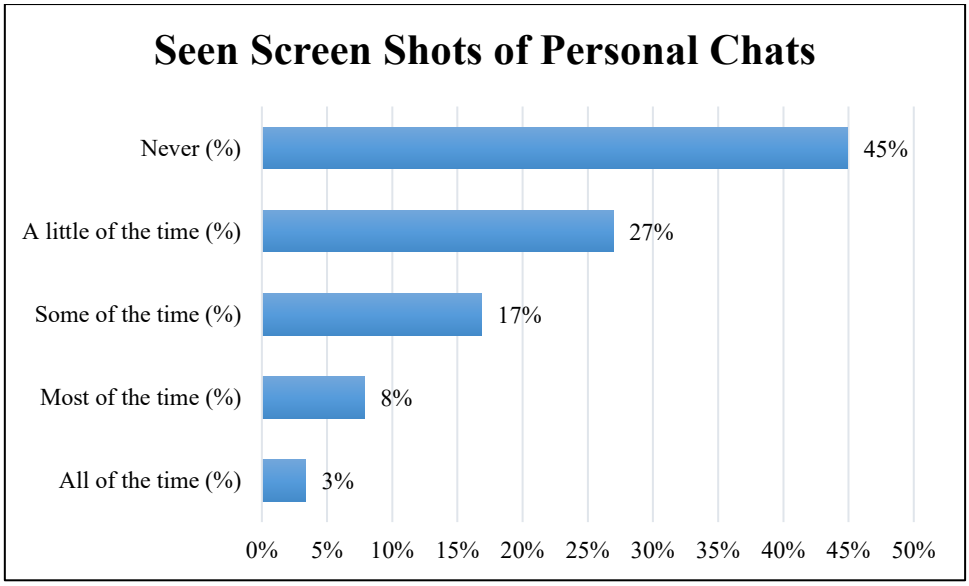


Figure 27: Seen Screen Shots of Other's Personal Chat

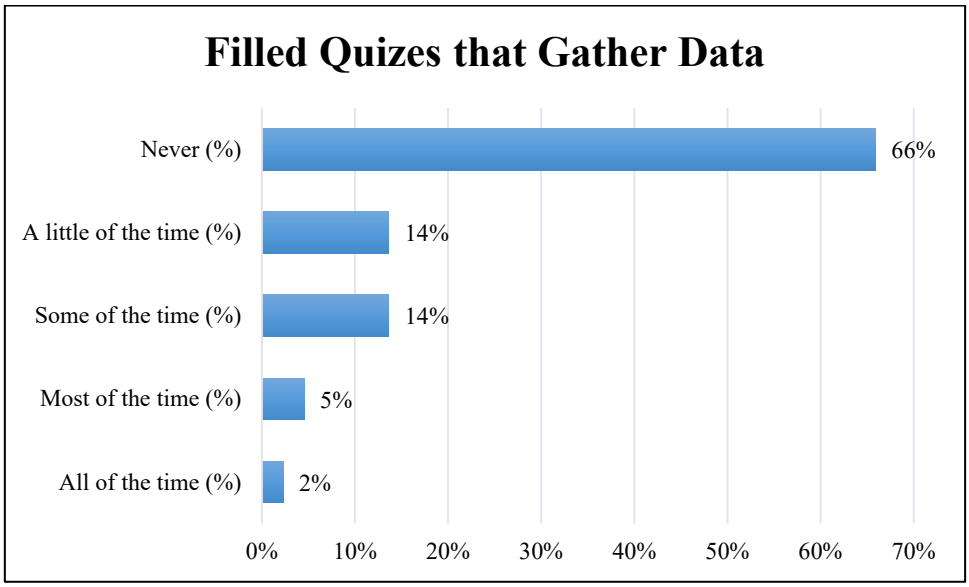


Figure 28: Filled Quizzes after providing Personal Info

42% of the sample have shared their personal information online, 15% even shared their passwords of different accounts online with others, 44% of them share their daily life events on social media and 5% are addicted to this habit, The rate of Disclosure of personal information is very high as 55% of the sample population has seen and read screen shots of personal chats of others. 34% of them have played different games and filled quizzes after giving their personal credentials for logging in.

5.5.5.2 Offline Contact Risk

This sub domain of contact risks category can be the most dangerous one as the risks which are present online can be materialized physically due to offline contact. When Children are asked do they have such friends those are unknown to them in real life 39% of them answered in Yes with different frequencies as shown in Table 14 and 15% have a habit of making online friends which are strangers in real life and actually unknown to them. 25% of them told that they have physically met their online unknown friends which is a quite dangerous situation for children.

Table 5-12: Offline Contact Risks

Offline Contact Risks								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 31	89	2	2%	13%	8%	16%	61%	100%
Question 32	88	3	2%	3%	2%	17%	75%	100%

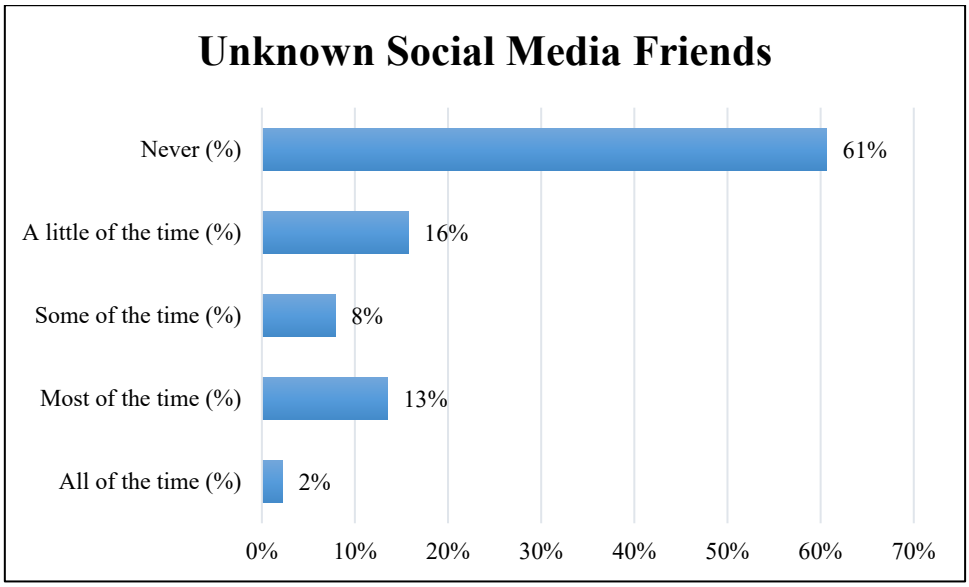


Figure 29: Unknown Social Media Friends

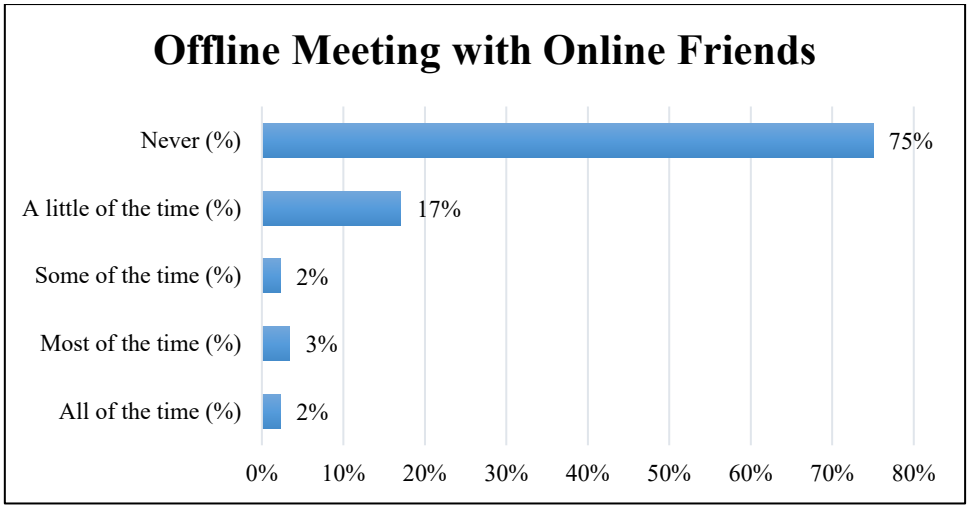


Figure 30: Physically Meeting Online Friends

5.5.6 Conduct Risks

The third category of internet risks in which child is personally involve in conducting all the misbehaviour described in above categories. This is further categorized in four sub domains.

5.5.6.1 Bullying and Harassing Others

13% children admitted to be involved in bullying others online.

Table 5-13: Conduct of Bullying

Conduct of Bullying								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 33	86	5	0%	0%	6%	7%	87%	100%

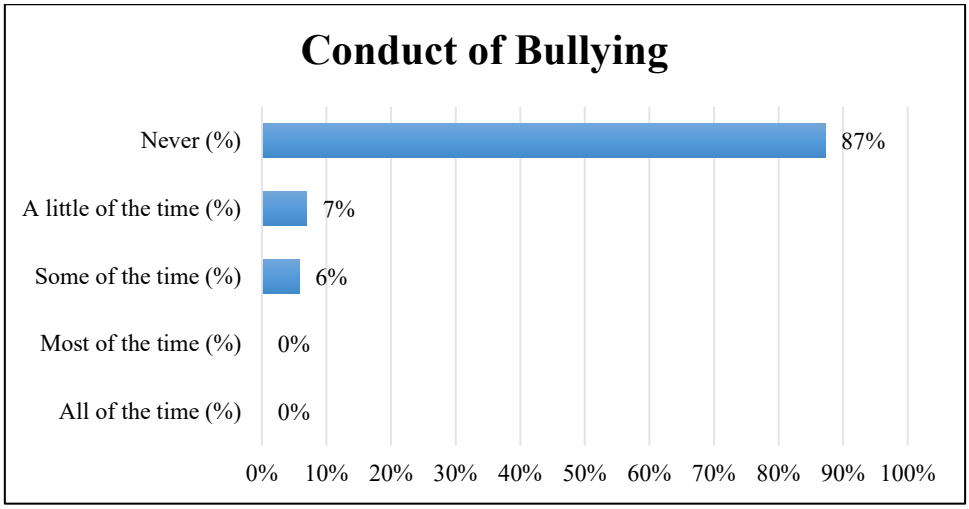


Figure 31: Conduct of Bullying

5.5.6.2 Conduct of Uploading Fake or Harmful Material

In response of two questions belonging to this category 8% children admitted of uploading, sharing or creating harmful material and 20% of children admitted to share fake news or incorrect information without authentication and involved in reposting such material without a reference. The data gathered in response of both measurement questions of this construct category is tabulated as under:

Table 5-14: Uploading Fake or Harmful Material

Uploading Fake or Harmful Material								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 34	88	3	0%	0%	7%	13%	81%	100%
Question 35	88	3	0%	1%	2%	5%	92%	100%

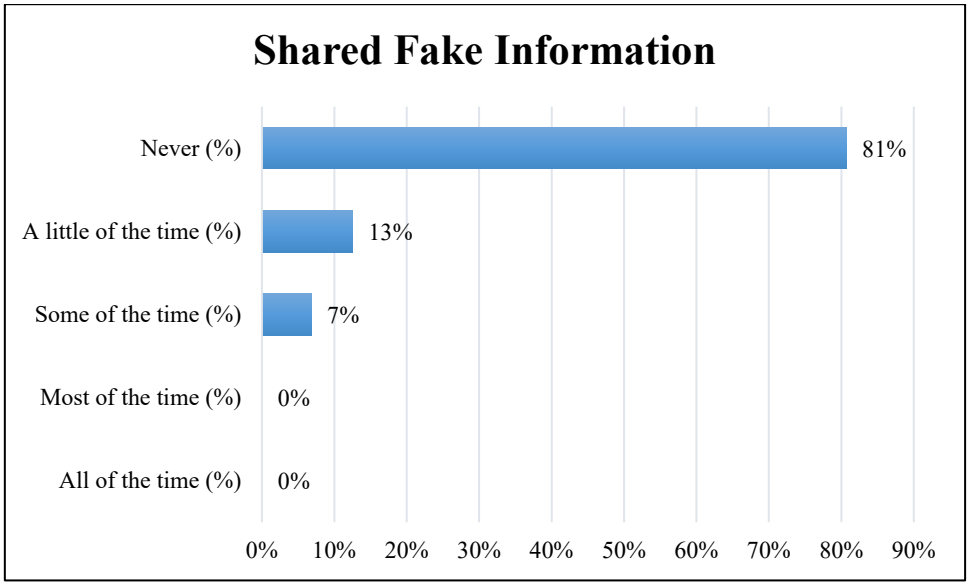


Figure 32: Sharing Fake Information

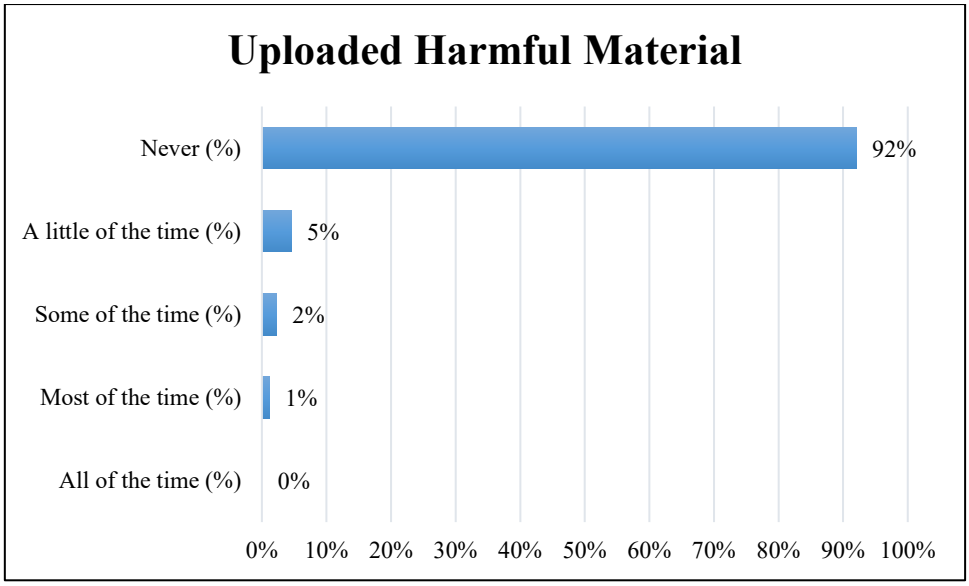


Figure 33: Uploaded Harmful Material

5.5.6.3 Privacy Risks

The privacy risks in Conduct risk category includes privacy breaching of others by your conduct i.e. by sharing screen shots etc. 16% of the targeted sample admitted to do so.

Table 5-15: Disclosing Privacy of Others

Privacy Risks								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 36	88	3	1%	0%	2%	13%	84%	100%

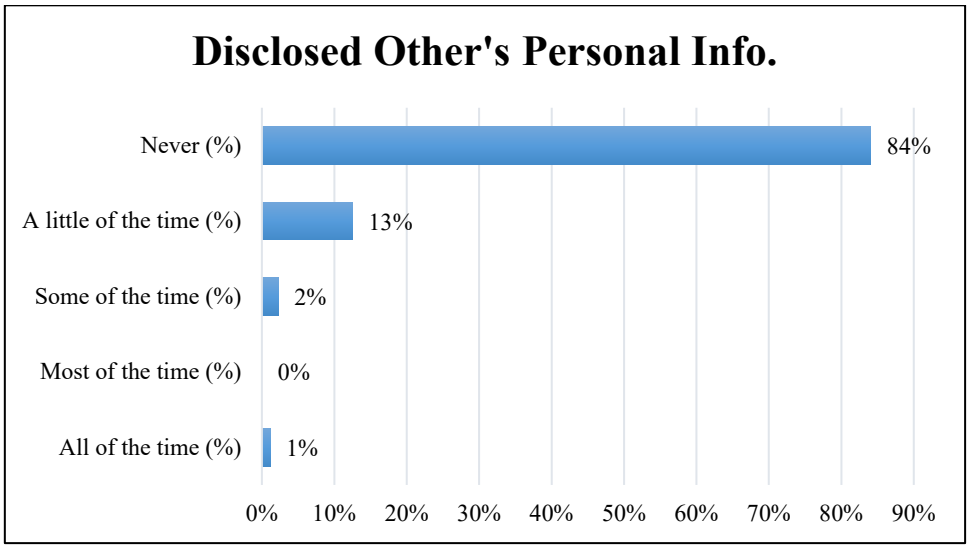


Figure 34: Disclosing Privacy of Others

5.5.6.4 Illegal Downloads

42% of children admitted to download pirated copies of books and pirated version of software and games and 20% of them committed it frequently.

Table 5-16: Illegal Downloads

Illegal Downloads								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 37	88	3	11%	9%	5%	17%	58%	100%

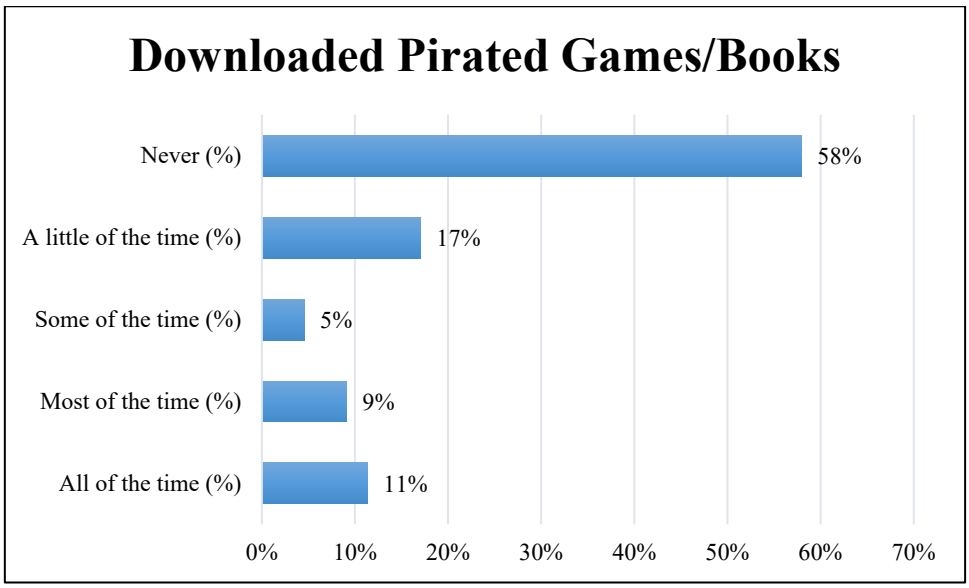


Figure 35: Illegal Downloads

5.5.7 Technological Risks

The fourth and last category of internet risks that measures risks that are not directly caused by human behaviour but by the means of technology. Results according to further categorization are as under.

5.5.7.1 Falling for Scams

Internet is full of scam offers of products and services. Children being netizens also came to face such fake deals and became a victim. 61% of the children reported for facing such scam offers and 20% of them used to see such offers with high frequency.

Table 5-17: Falling for Scams

Falling for Scams								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 38	88	3	2%	18%	19%	22%	39%	100%

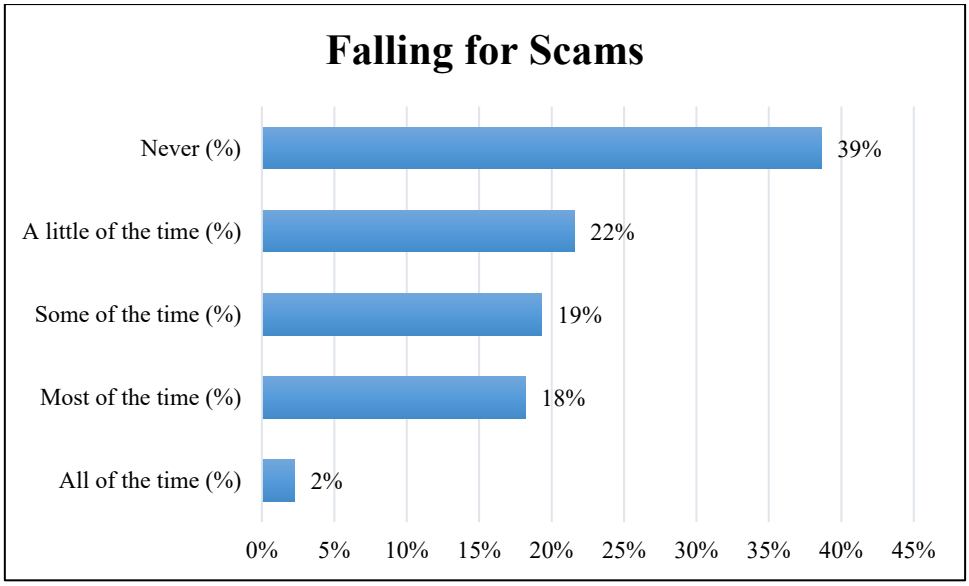


Figure 36: Falling for Scams

5.5.7.2 Accidently Downloading Malware

Accidently downloading a malware is the most common and highly occurring sub category of technological risks domain of internet risk categorization. 45% of the children told that they have accidently downloaded a malware by clicking a random pop up message or link that appear on their screens while using internet for different purposes. 72% of them have downloaded such games that are actually adware and 26% have conducted such downloads frequently. This is a very high percentage which shows that this is the most common technological risk faced by children. 47% reported data corruption due to certain game downloads. Children downloaded games that are not actually the games but malware and make them in huge trouble by corrupting all the data present on that device on which download has been done. The data is tabulated and presented below:

Table 5-18: Accidentally downloading a Malware

Accidentally Downloading a Malware								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 39	87	4	1%	5%	16%	23%	55%	100%
Question 40	88	3	3%	23%	23%	23%	28%	100%
Question 41	88	3	2%	3%	20%	20%	53%	100%

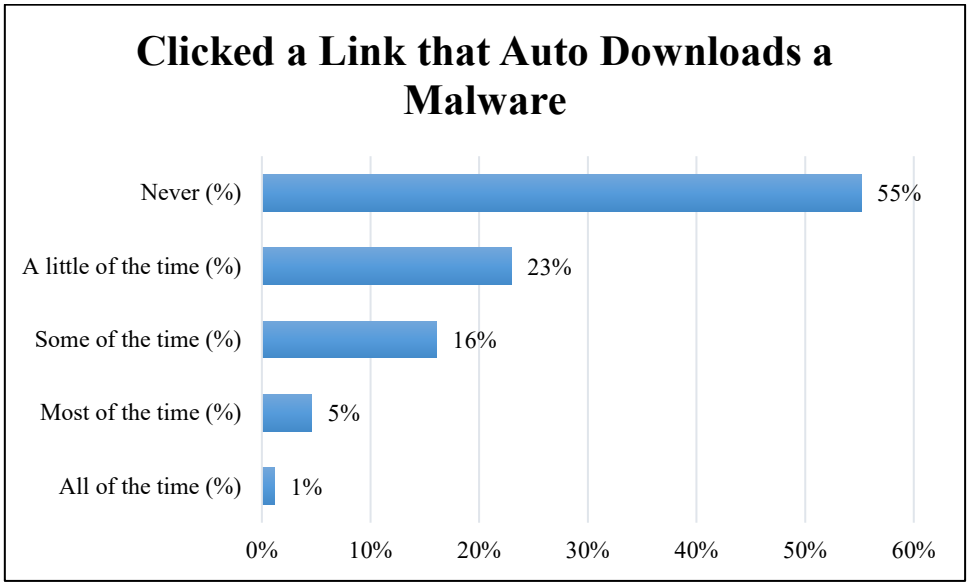


Figure 37: Auto Download of Malware

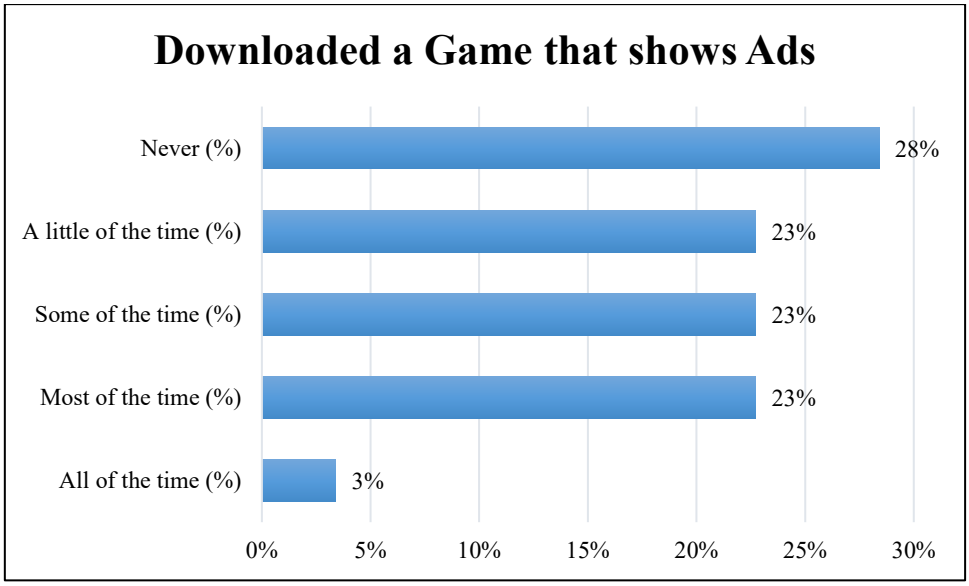


Figure 38: Games as Adware

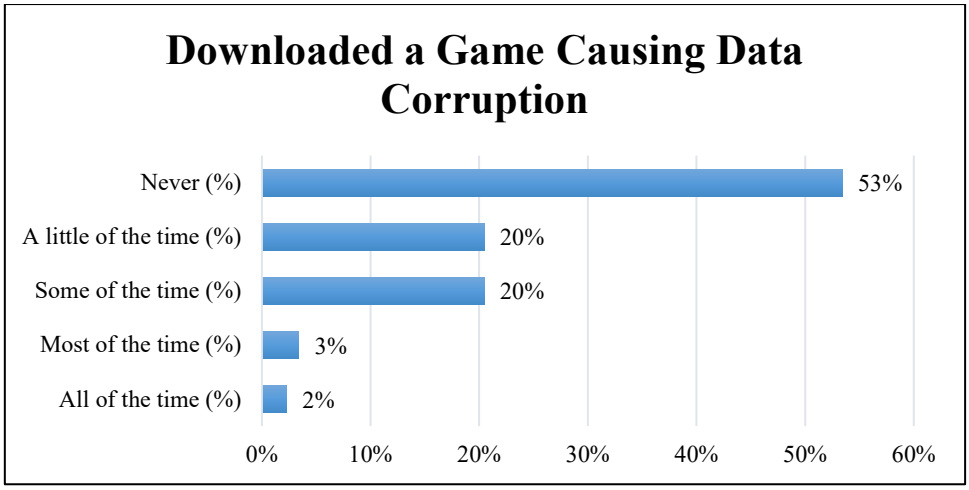


Figure 39: Game Causing Data Corruption

5.5.7.3 Phishing

This technological risk seems to be least occurring according to the results as 41% of children has experienced receiving emails that ask to click such links that consequently redirects them to malicious pages. 38% of them had received phishing emails and only 18 % reported to receive such messages.

Table 5-19: Phishing

Phishing								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 42	88	3	2%	2%	14%	23%	59%	100%
Question 43	89	2	1%	1%	9%	27%	62%	100%
Question 44	89	2	0%	2%	3%	12%	82%	100%

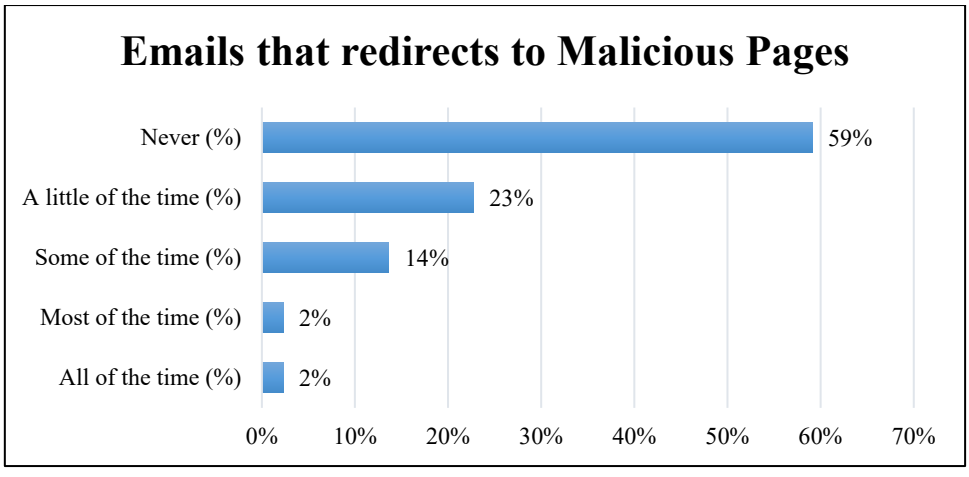


Figure 40: Email Redirecting to Malicious Pages

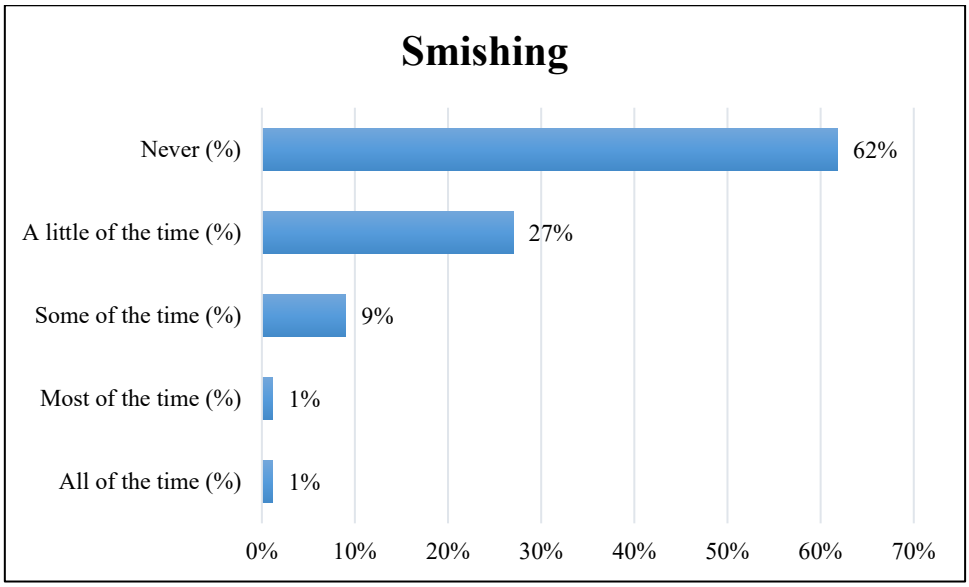


Figure 41: Smishing

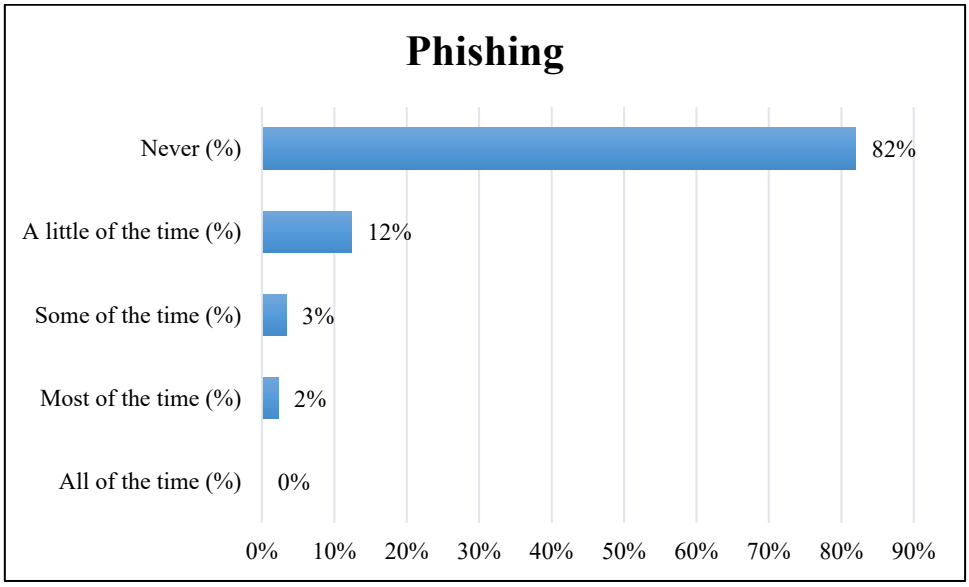


Figure 42: Phishing

5.5.8 Miscellaneous Questions

After measuring about internet risk categorization children were asked to miscellaneous questions at the end.

5.5.8.1 Most Negative Impact

The important one from them was asking about most negative impact of the internet risk situations in which 25% of the people have reported that the were disturbed most by the fake news spread on the internet. Second most reported category is Online Harassment which is one

of the worst online risks. 21% of the children have reported this as having worst effects on young mind. At third place 14% of the targeted sample told that adult/violent content has most negative impact on their young minds 10% reported for both disclosure of personal data and for religious hatred and provincial bigotry. At last place 9% of the children reported bullying as the worst happening online risk to them.

Table 5-20: Most Negative Impact

Most Negative Impact										
Questions	Total Responses	Blank Answers	Bullying (%)	Harassment (%)	Violent/ Adult content (%)	Religious hatred/ Provincial bigotry (%)	Fake news (%)	Disclosure of personal data (pictures etc.)	Accidentally downloading a virus (%)	TOTAL (%)
Question 45	87	4	9%	21%	14%	10%	25%	10%	10%	100%

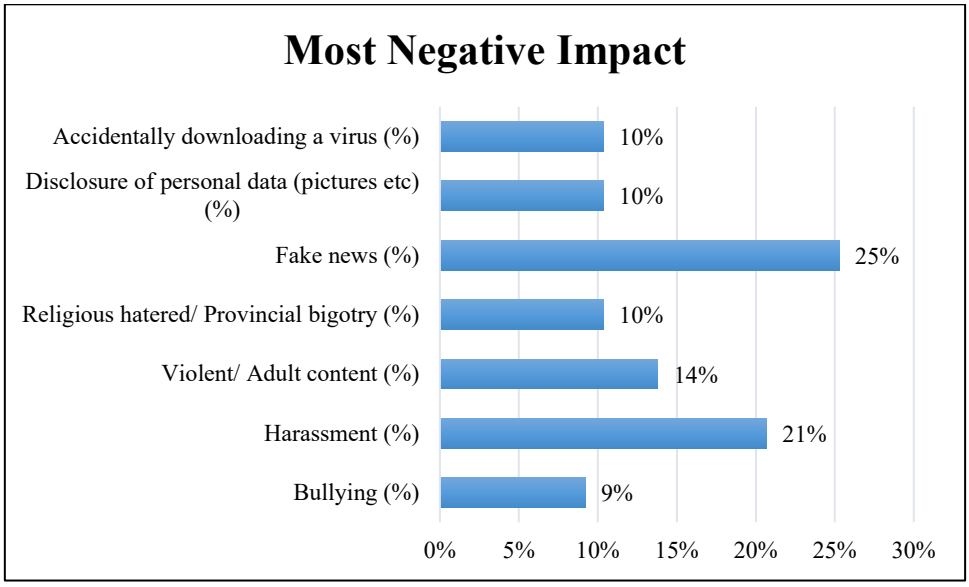


Figure 43: Most Negative Impact

5.5.8.2 Seek for Guidance

The last question of the questionnaire was intended to measure if the children have asked for proper guidance after suffering from any unwanted online risk situation or not. 72% of them had answered in agreement which is favourable condition.

Table 5-21: Seek for Proper Guidance

Seek for Proper Guidance								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 46	88	3	9%	16%	18%	28%	28%	100%

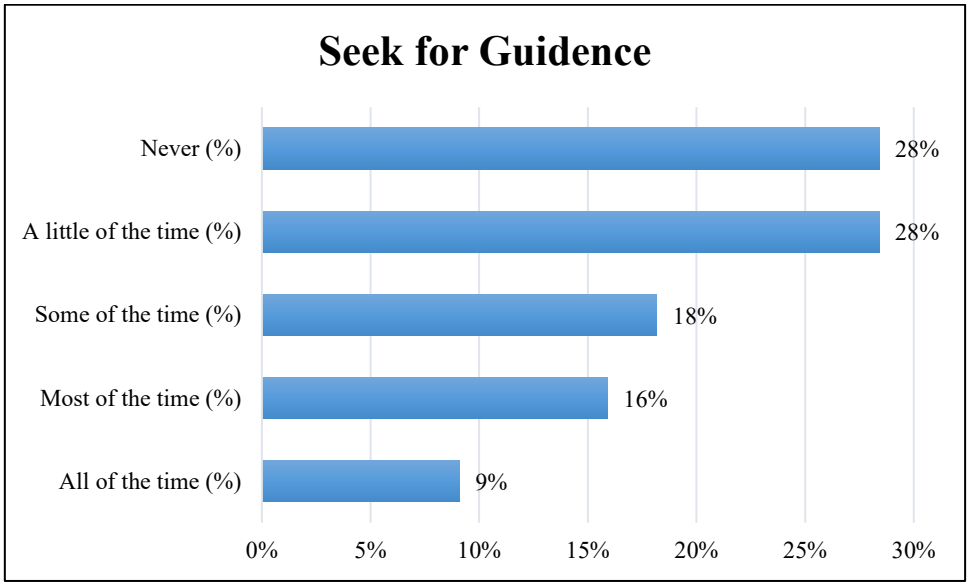


Figure 44: Seek for Proper Guidance

5.6 RESULTS AND FINDINGS OF OFFLINE SURVEY:

After scaling and filtering the raw data into meaning full data, the tabulation and graphing process have been done. The data have been categorized into subsets according to the designed constructs as discussed in the previous chapter. Following are the details of gathered data:

5.6.1 BASIC INTERNET USAGE:

Table 5-22: Data of basic Internet Usage

Questions	Construct	TOTAL	BLANK ANSWERS	YES (%)	NO (%)	TOTAL (%)
Question 2	Internet facility	**56**	4	66%	34%	**100%**
Question 3	Webcam	**57**	3	84%	16%	**100%**
Question 5	Internet outside Homes & Schools	**58**	2	44%	56%	**100%**
Question 6	Access to Social Media	**58**	2	26%	74%	**100%**
Question 7	Personal Social Media Accounts	**55**	5	28%	72%	**100%**

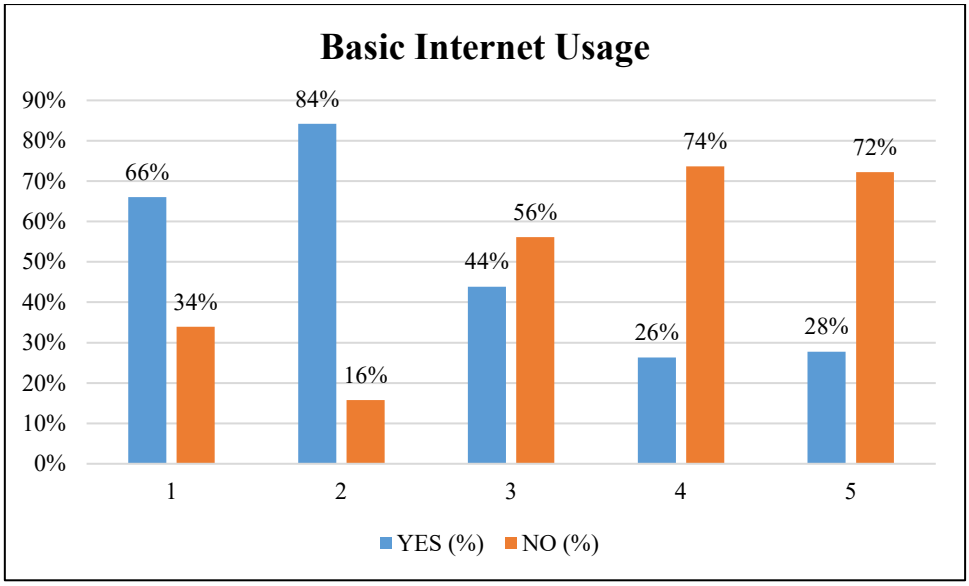


Figure 45: Basic Internet Usage

The first Categorization after initial introduction questions in the designed questionnaire was about to measure basic internet usage of the target population. How familiar are they with the internet devices and how many have access to the online platforms. Results shows that 66 % children are using Webcam, 84% of them had internet facility and 44% have this facility outside school and homes as well. As for social media usage 26% of them has access to social media accounts of their own or parents or siblings while when asked about their own social media accounts than this percentage astonishingly increases to 28%. Next table shows the percentage in hours of how much time children spend on internet daily.

Table 5-23: Time Spent on Internet (in hours)

Internet Usage	No of Responses	Percentages
Up to 3 hours (%)	35	**69%**
3 to 6 hours (%)	8	**16%**
6 to 9 hours (%)	3	**6%**
9 to 12 hours (%)	2	**4%**
More than 12 hours (%)	3	**6%**
TOTAL (%)	51	**100%**

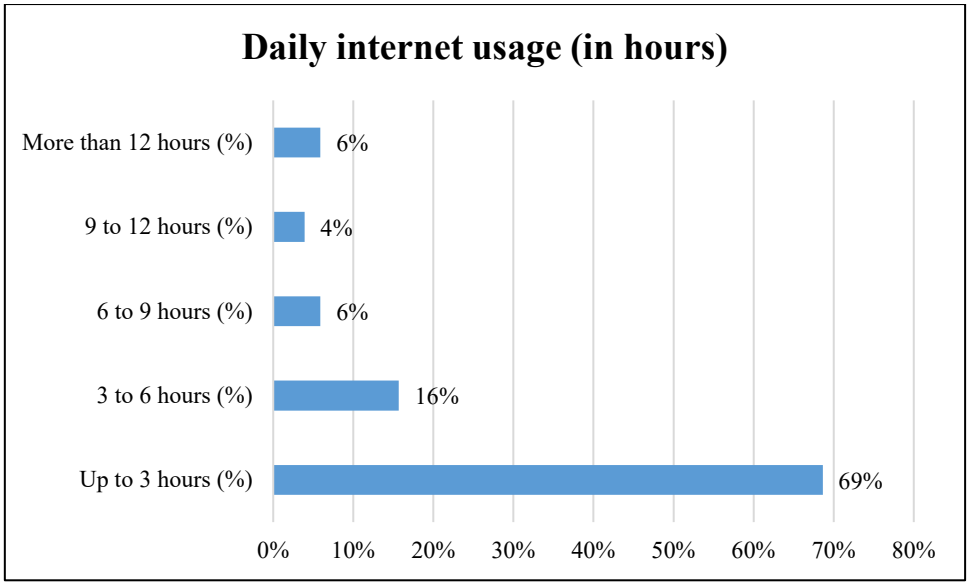


Figure 46: Daily Internet Usage in hours

The statistics shows that about half of the population of targeted sample i.e. 69% spend limited time on internet that is up to 3 hours per day, and half of the remaining half i.e. 16% spend up to 6 hours daily online while the remaining population although less in number but their internet usage time increases. 6% of them spend more than quarter of a day online i.e. up to 9 hours, 4% spent almost 12 hours it means half of a day and online. And there are 6% severe cases who spent more than half of their day on internet.

5.6.2 BASIC LEVEL OF AWARENESS

The next categorization includes questions about basic level of internet risks awareness. The gathered data is tabulated as under.

Table 5-24: Basic level of Cyber Security Awareness

Questions	Construct	TOTAL	BLANK ANSWERS	YES (%)	NO (%)	TOTAL (%)
Question 8	Activated Security Settings	**58**	2	69%	31%	**100%**
Question 9	Aware of Unsafe Internet Usage	**58**	2	79%	21%	**100%**
Question 10	Online stuff is Inerasable	**57**	3	49%	51%	**100%**
Question 11	Briefing about Online Safety	**57**	3	67%	33%	**100%**

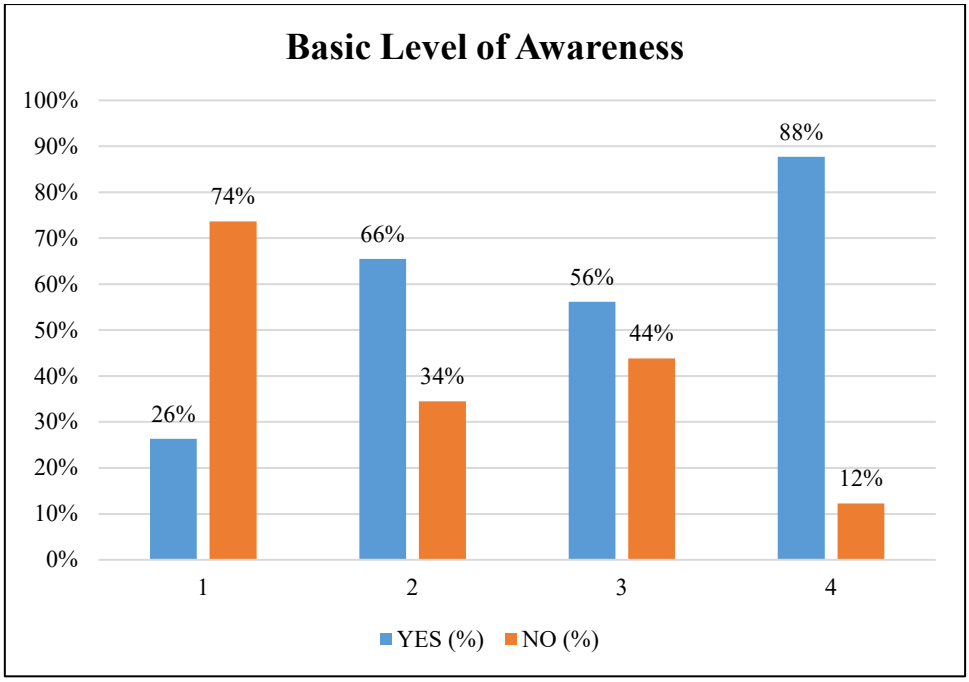


Figure 47: Basic Level of Awareness

The responses shows that only 26% of children in targeted sample have activated security settings provided by the social media developers, 66% told that they are familiar with harms and threats of unsafe internet usage, but only 56%, less than half, knows that the material once posted online can never be erased, and 88% were briefed by their parents or teachers about internet risks.

5.6.3 Content Risks

Internet Risk Categorization starts from here. Initially internet risks are divided into four categories. The first one is Content Risks. This category is further divided into sub domains namely Provocative Content, Incorrect Content and Commercial Content. Further categorization makes the construct which are measured in the questionnaire and results and findings are discussed below accordingly.

5.6.3.1 Age Inappropriate Content

Age inappropriate risk is the first construct from this category. Following is the data of three questions related to this construct.

Table 5-25: Data of Age Inappropriate Content

Age Inappropriate Content								
Questions	**TOTAL**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 11	**91**	0	2%	7%	16%	23%	52%	**100%**
Question 12	**88**	3	0%	9%	24%	28%	39%	**100%**
Question 13	**91**	0	0%	3%	13%	19%	65%	**100%**

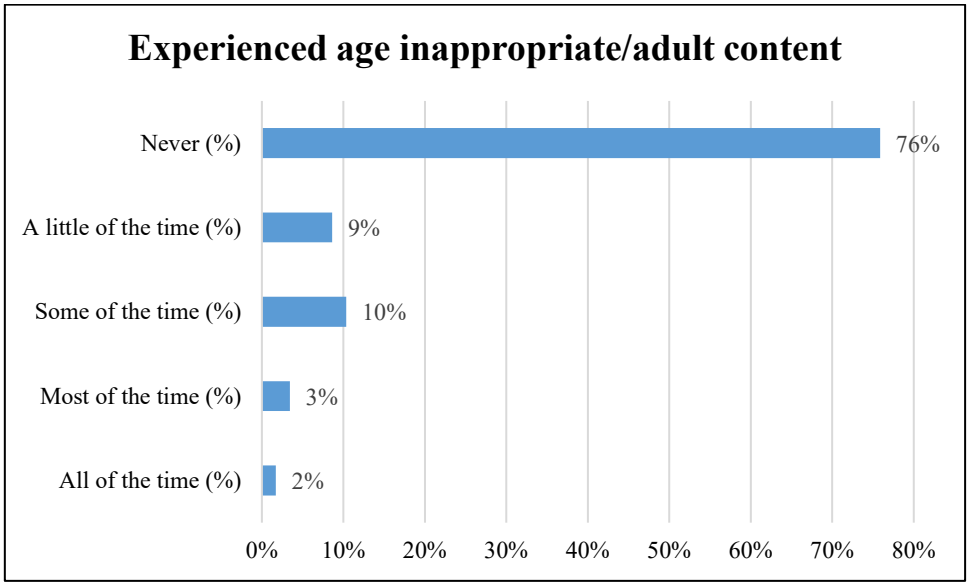


Figure 48: Experienced Age Inappropriate Content

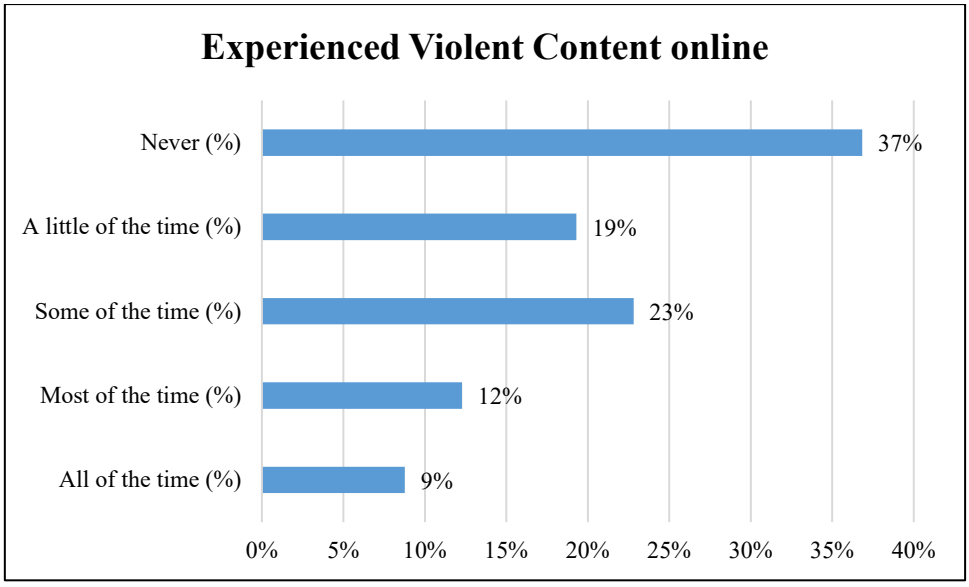


Figure 49: Experienced Violent Content

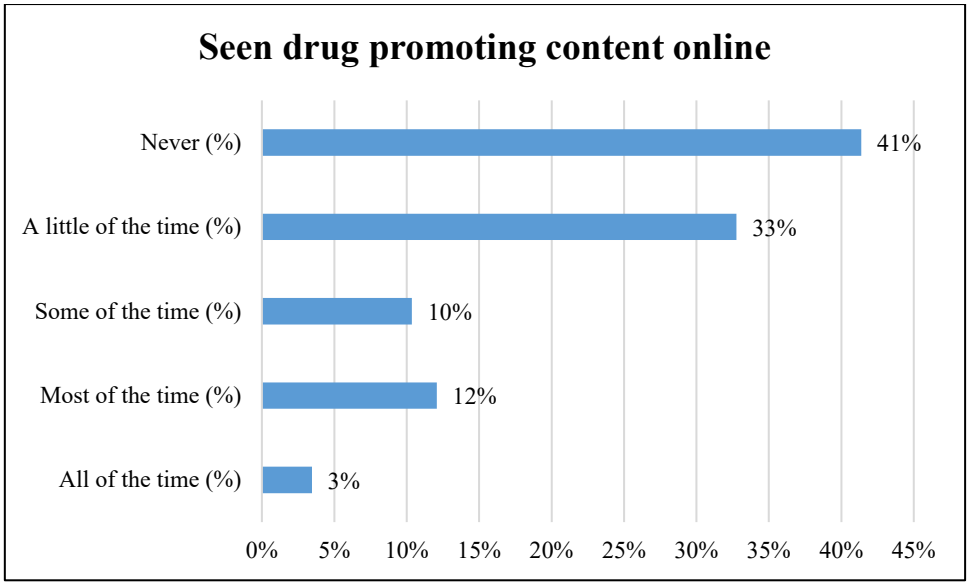


Figure 50: Drug Promoting Content

Above figures show the data of children who have experienced the three kinds of age inappropriate content i.e. adult, violent or drug promoting content in which frequency. Many of the children replied as 'Never' but still there is a large number i.e. 48% who have experienced this kind of unwanted content. Violent content is the most experienced i.e. 61% from all the three types of Age inappropriate content. Drug promotions are seen by 35% of students.

5.6.3.2 Content Promoting Bias and Bigotry

Two questions were included in the questionnaire to measure content promoting bias and bigotry. The results are tabulated below.

Table 5-26: Content Promoting Bias and Bigotry

Content Promoting Bias and Bigotry								
Questions	**TOTAL**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 15	57	3	5%	25%	28%	18%	25%	100%
Question 16	58	2	3%	33%	12%	19%	33%	100%

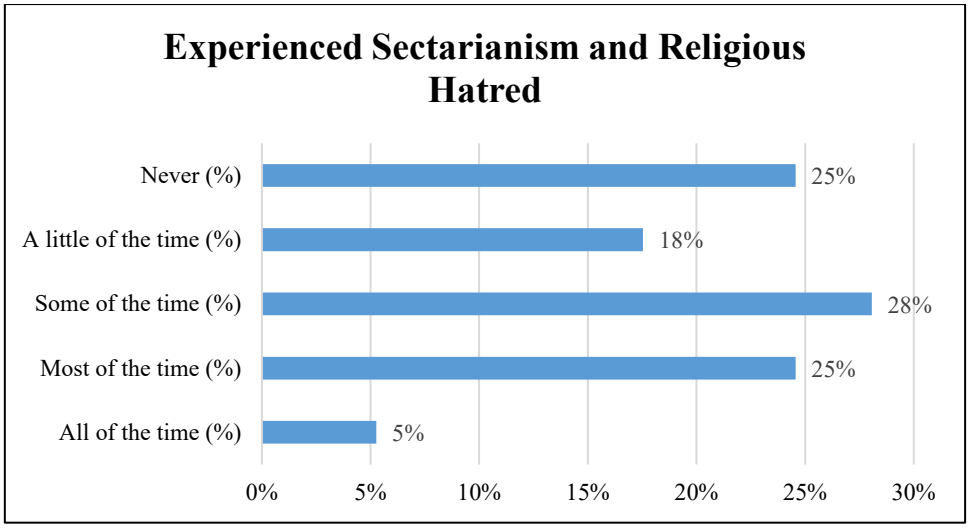


Figure 51: Experienced Sectarianism

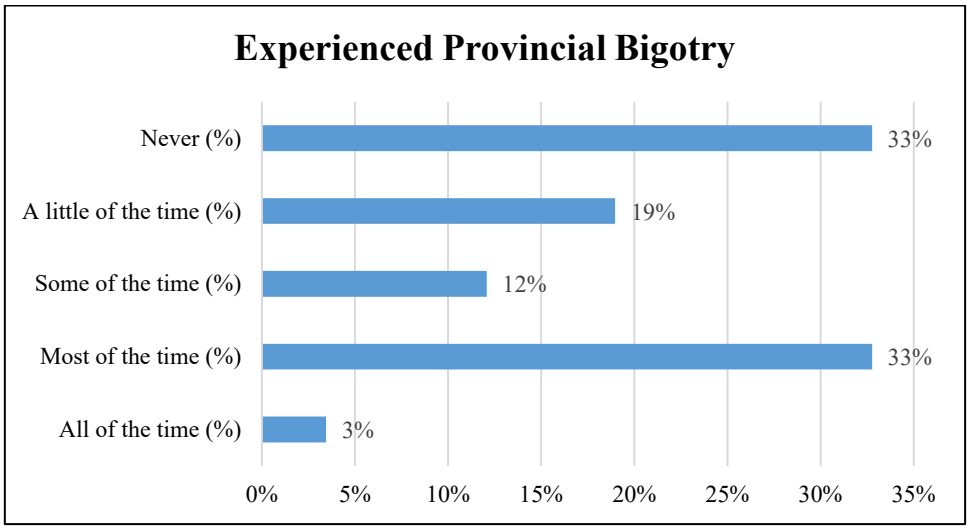


Figure 52: Experienced Provincial Bigotry

The first question about this construct was related to sectarianism and religious hatred and the second one was intended to measure provincial and linguistic bigotry. A very large population, i.e. 75% and 64% of the children in the target population has seen posts related to sectarianism and provincial bigotry respectively.

5.6.3.3 Incorrect Content

False information and Fake news are one of the most common content risk available online. And the results shows that the internet risk from which children are affected the most is Fake news. According to survey 86% of the targeted sample population of the children has experienced this internet risk.

Table 5-27: Fake or Incorrect Information

Fake News or False Information								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 17	90	1	19%	39%	21%	11%	10%	100%

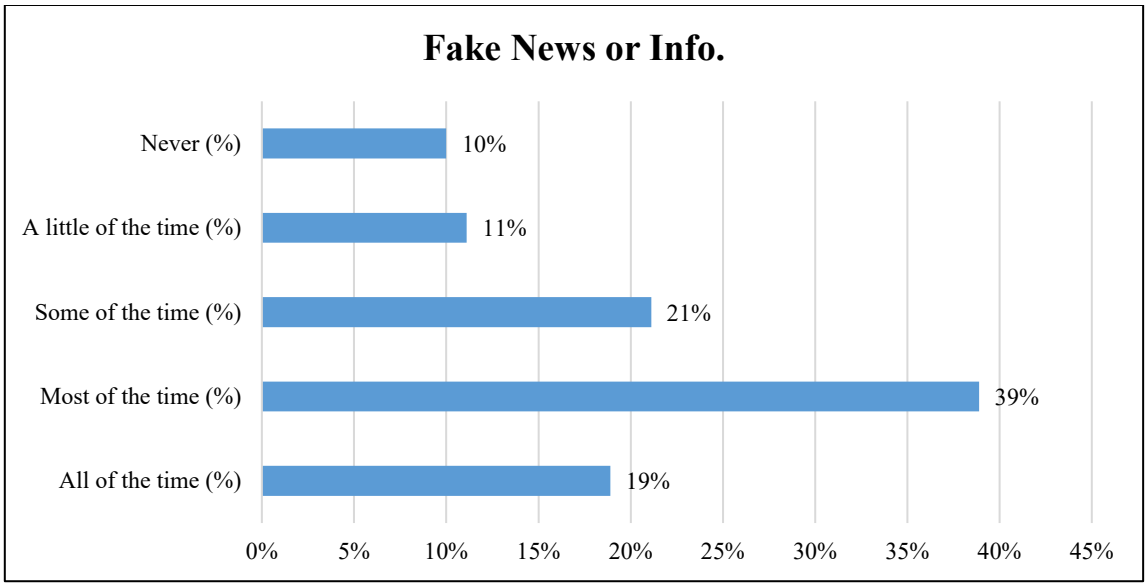


Figure 53: Fake news or Info.

The Results shows high suffering of the children from False and Incorrect information that become viral on internet without authentication and reference. As in current pandemic situation fake notifications about opening and closure of schools became viral.

5.6.3.4 Commercial Exploitation

Commercial content is also one of the most occurring content risk on social media platforms and other web sites. Three questions have been included to measure its occurring intensity and the results are tabulated as under:

Table 5-28: Commercial Content

Commercial Exploitation								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 18	57	3	4%	18%	11%	12%	56%	100%
Question 19	58	2	0%	5%	7%	21%	67%	100%
Question 20	58	2	0%	5%	9%	14%	72%	100%

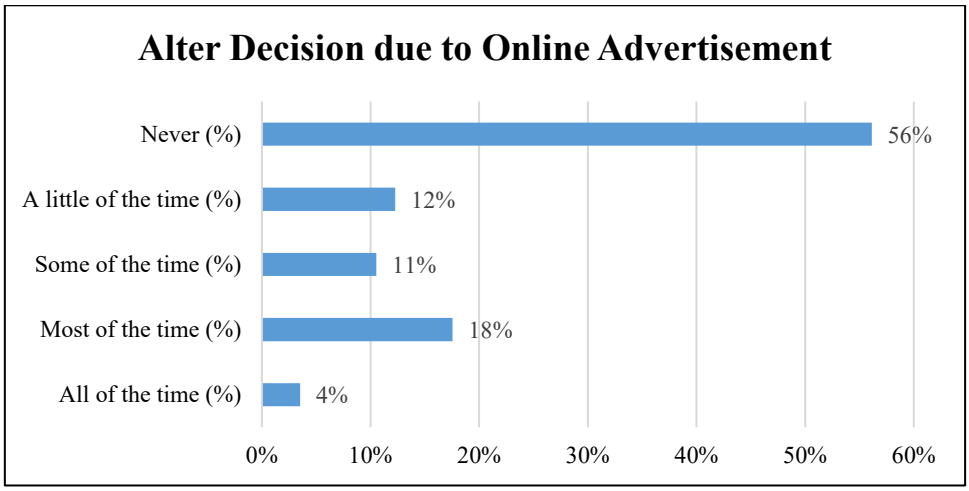


Figure 54: Decision change due to online Advertisements

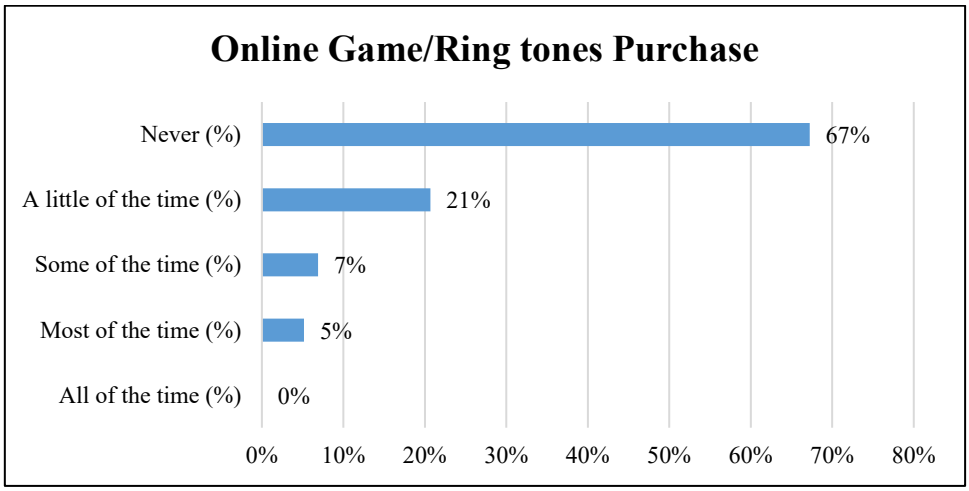


Figure 55: Online Games/ Ring Tones Purchase

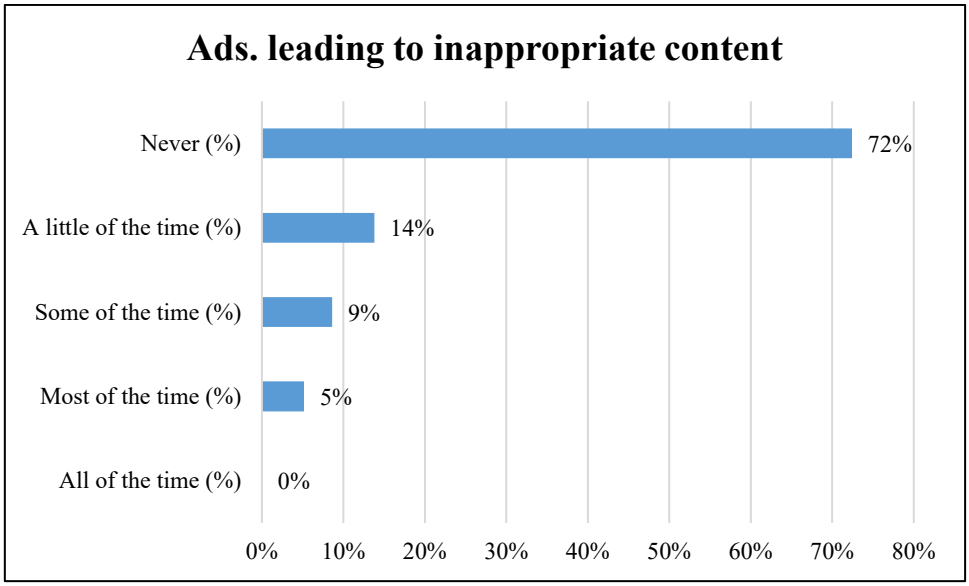


Figure 56: Advertisements Leading to Inappropriate Content

44% of the children have altered their decision due to online advertisements, percentage of purchasing of online games or ringtones is quite low but still 33% of children still gone through this. And the highest risk category in this domain is in which advertisements lead to inappropriate content. 28% of the targeted sample has faced this risk in different frequencies as shown in the graph.

5.6.3.5 Unwanted Collection of Personal Data

The last sub domain of content risk is unwanted collection of personal data. In this domain children are asked for giving their personal data for subscription of games or home-work websites etc. This was measured by one question and the results show that more than half i.e. 24% of targeted children have got such subscriptions.

Table 5-29: Unwanted Collection of Data

Unwanted Collection of Personal Data								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 21	58	2	0%	3%	14%	7%	76%	100%

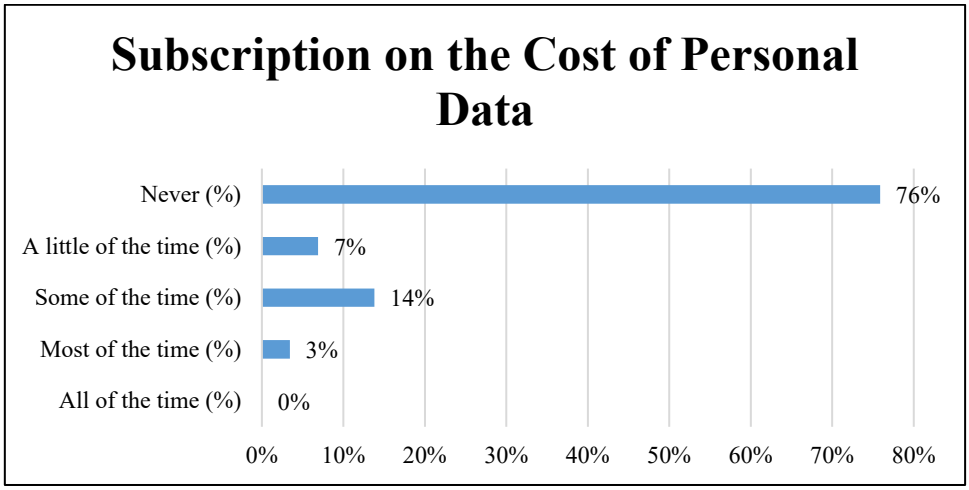


Figure 57: Unwanted Collection of Data

5.6.4 Contact Risks

Second domain of Human Risks is Contact risks.

5.6.4.1 Cyber Bullying

It is the first and most common sub category of Contact Risks domain. The result of three measurement questions is as under:

Table 5-30: Cyber Bullying

Cyber Bullying								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 22	58	2	0%	9%	16%	28%	48%	100%
Question 23	58	2	0%	3%	10%	10%	76%	100%
Question 24	58	2	10%	21%	17%	10%	41%	100%

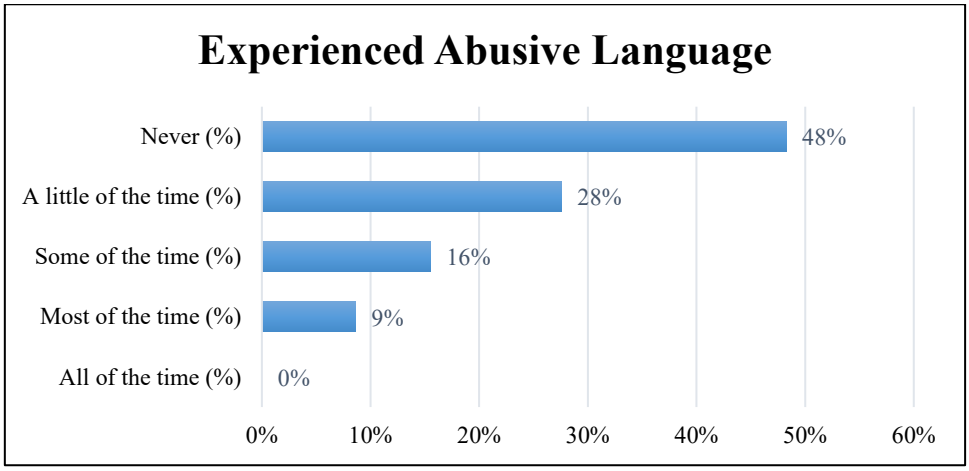


Figure 58: Faced Abusive Language

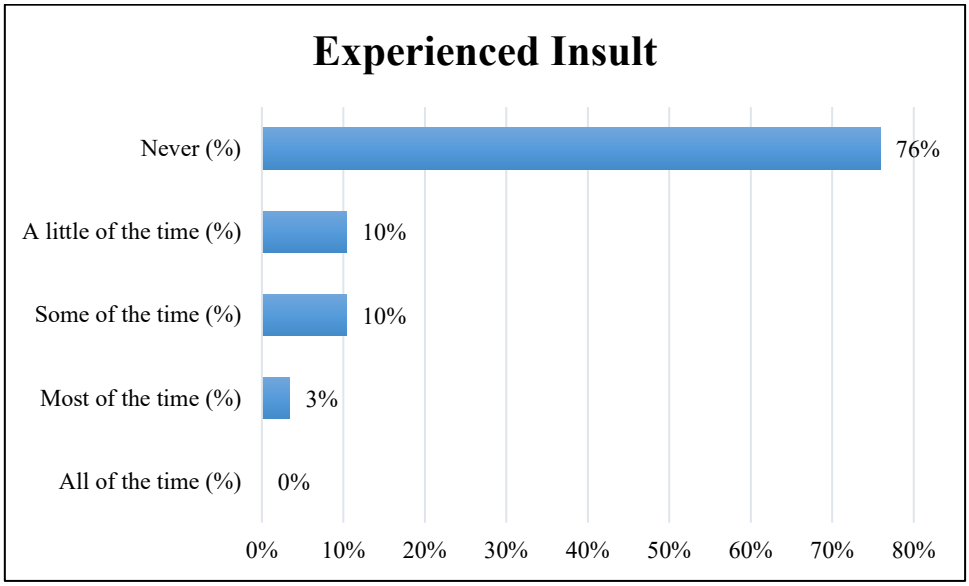


Figure 59: Felt Humiliation Online

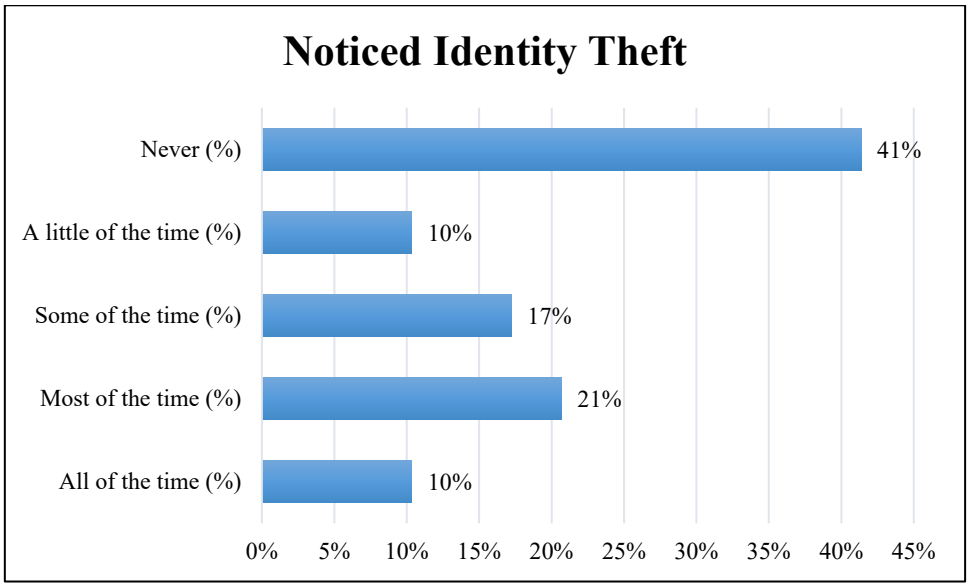


Figure 60: Noticed Fake Profiles

52% of children have faced abusive language, 24% of them has felt humiliated due online negative behaviors of other and 59% of them have noticed identity theft and fake profiles which is a large number.

5.6.5 Sexual Solicitation

The most unethical and unwanted contact risk is sexual exploitation. And 26% of the students reported to experienced online harassment.

Table 5-31: Online Harassment

Online Harassment								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 25	58	2	0%	2%	12%	10%	76%	100%

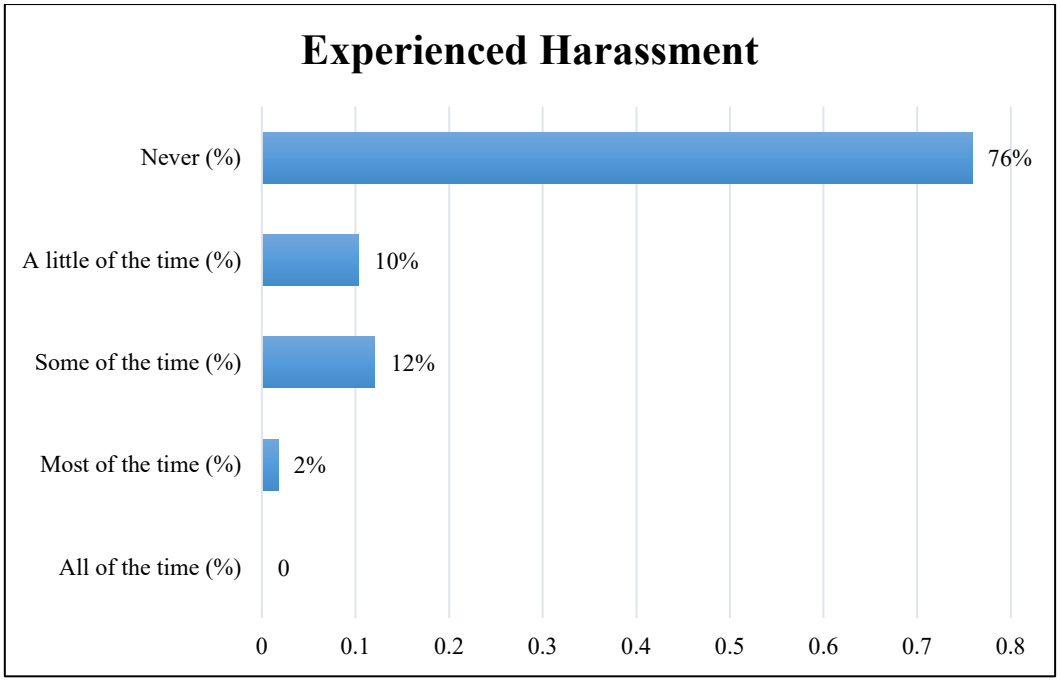


Figure 61: Experienced Harassment

5.6.5.1 Uploading Personal Information

This is the broadest category of contact risks. The questionnaire included five questions to measure all the aspects like uploading personal information as name, home addresses, email addresses, school name etc. and sharing password with others or sharing personal and family pictures. Results are tabulated below.

Table 5-32: Uploading Personal Information

Uploading Personal Information online								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 26	58	2	0%	5%	5%	14%	76%	100%
Question 27	58	2	0%	0%	5%	10%	84%	100%
Question 28	58	2	3%	7%	12%	9%	69%	100%
Question 29	58	2	3%	0%	14%	28%	55%	100%
Question 30	58	2	0%	12%	19%	14%	55%	100%

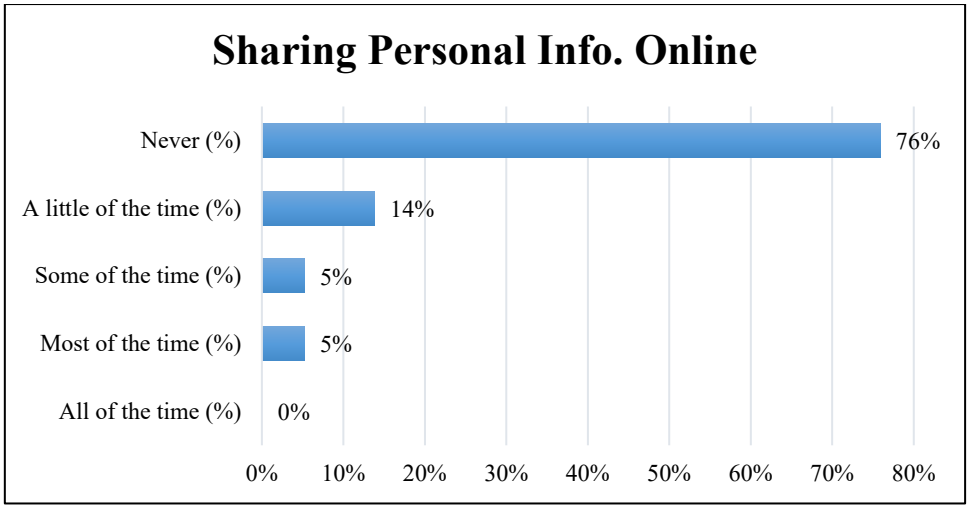


Figure 62: Shared Personal Information

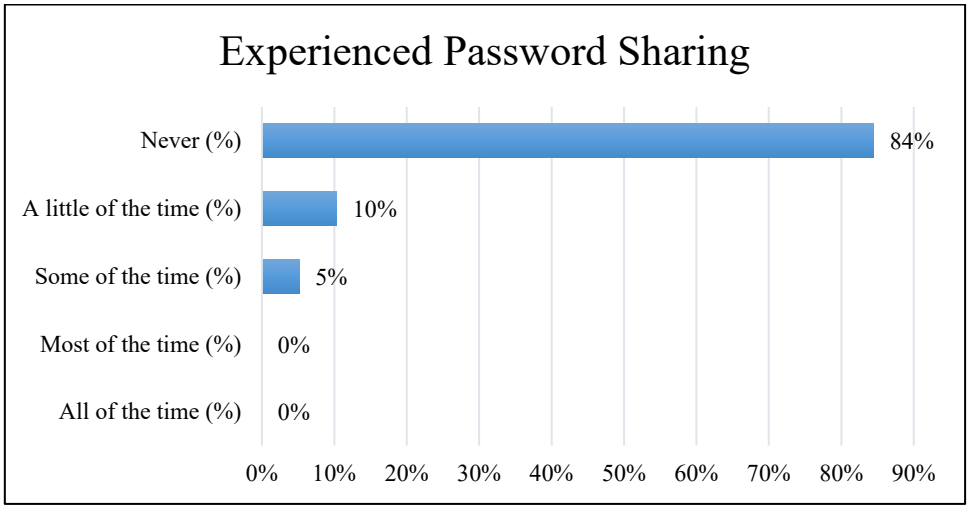


Figure 63: Shared Password with Someone

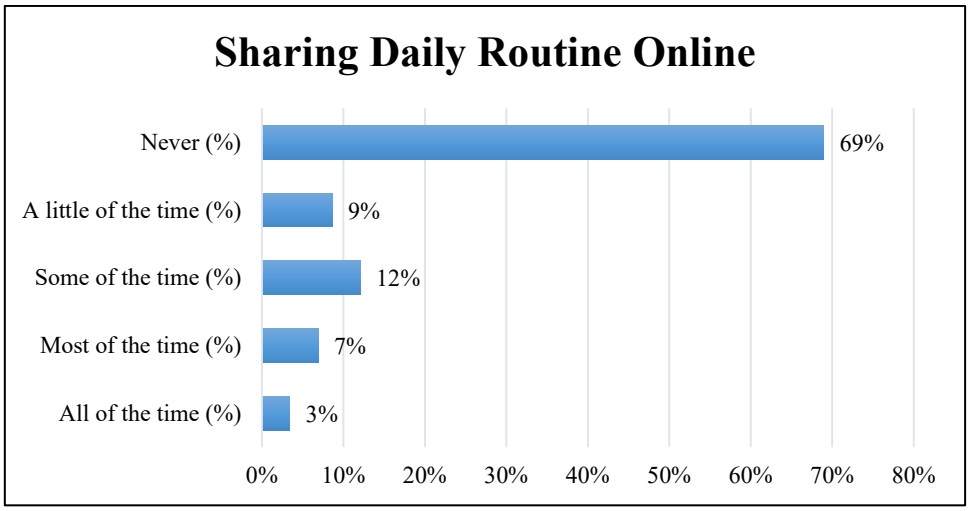


Figure 64: Shared Daily Routine

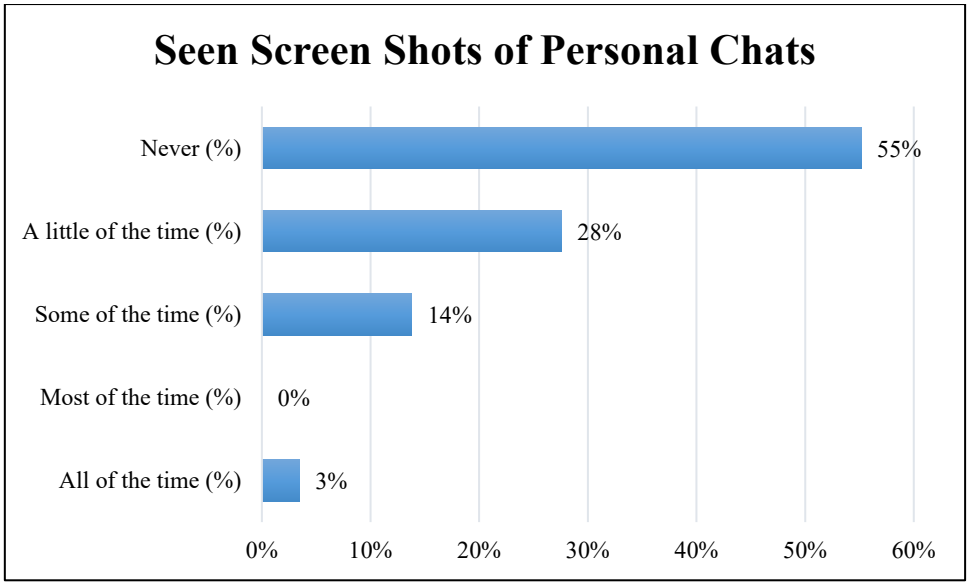


Figure 65: Seen Screen Shots of Other's Personal Chat

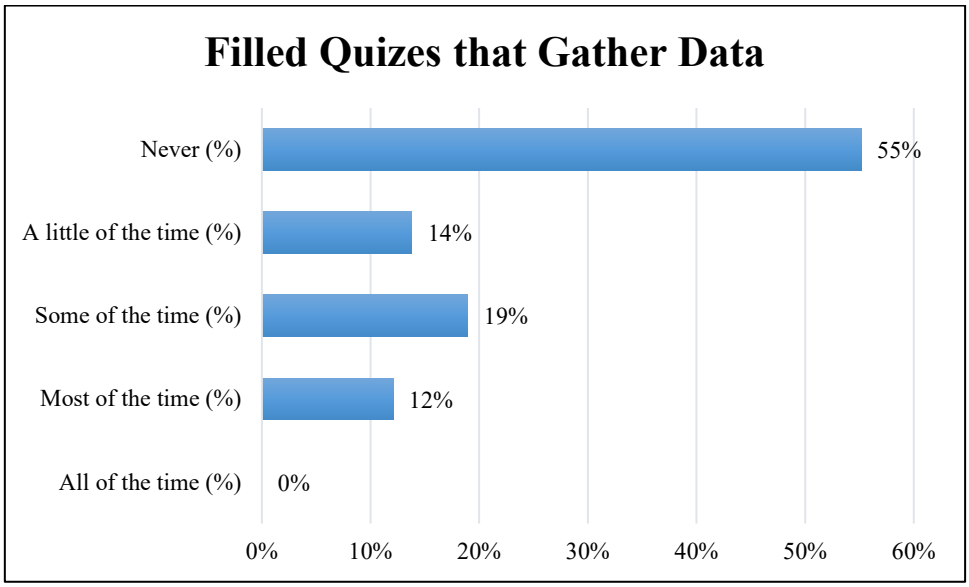


Figure 66: Filled Quizzes after providing Personal Info

24% of the sample have shared their personal information online, 26% even shared their passwords of different accounts online with others, 31% of them share their daily life events on social media and 10% are addicted to this habit, The rate of Disclosure of personal information is very high as 45% of the sample population has seen and read screen shots of personal chats of others. 45% of them have played different games and filled quizzes after giving their personal credentials for logging in.

5.6.5.2 Offline Contact Risk

This sub domain of contact risks category can be the most dangerous one as the risks which are present online can be materialized physically due to offline contact. When Children are asked do they have such friends those are unknown to them in real life 31% of them answered in Yes with different frequencies as shown in Table 35 and 15% have a habit of making online friends which are strangers in real life and actually unknown to them. 11% of them told that they have physically met their online unknown friends which is a quite dangerous situation for children.

Table 5-33: Offline Contact Risks

Offline Contact Risks								
Questions	**Total Responses**	**Blank Answers**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 31	58	2	0%	5%	7%	9%	79%	100%
Question 32	57	3	0%	2%	4%	5%	89%	100%

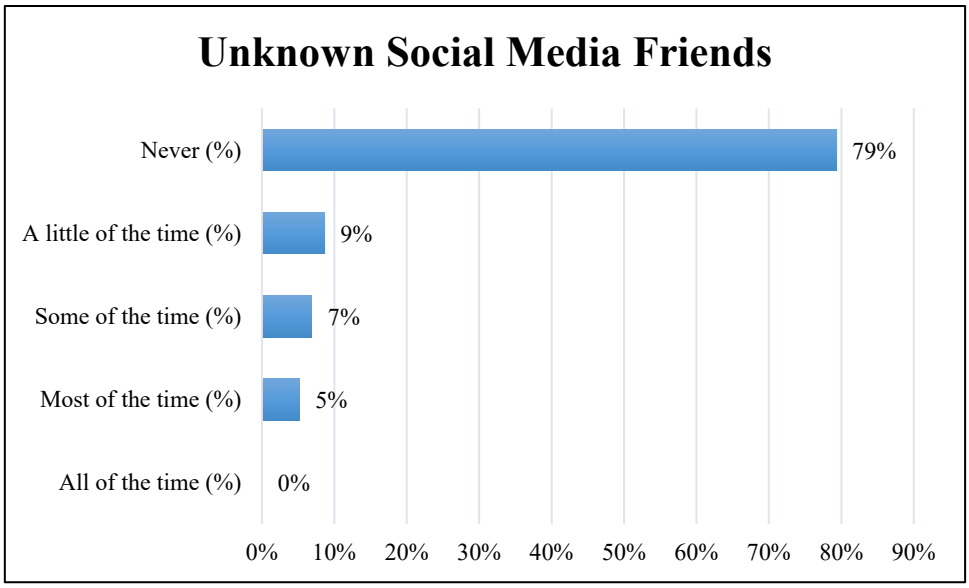


Figure 67: Unknown Social Media Friends

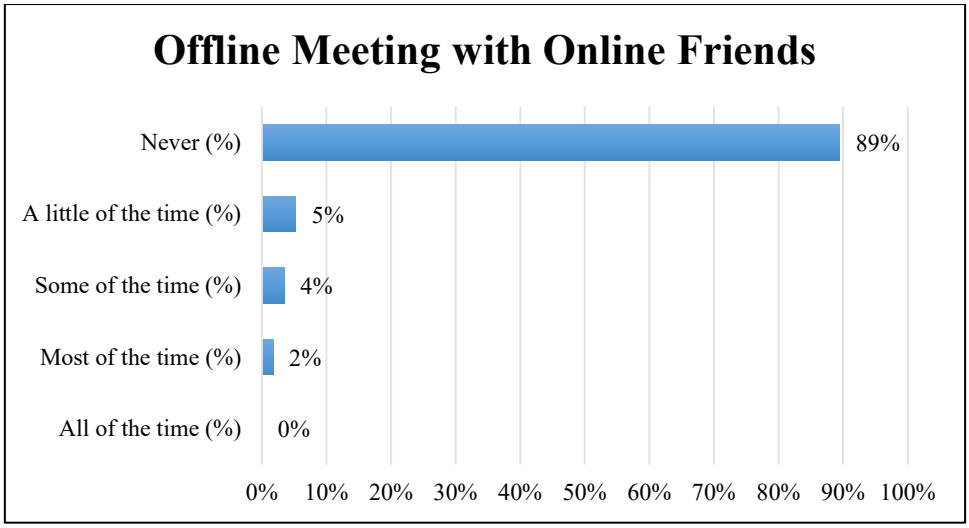


Figure 68: Physically Meeting Online Friends

5.6.6 Conduct Risks

The third category of internet risks in which child is personally involve in conducting all the misbehaviour described in above categories. This is further categorized in four sub domains.

5.6.6.1 Bullying and Harassing Others

Alarmingly 25% children admitted to be involved in bullying others online.

Table 5-34: Conduct of Bullying

Conduct of Bullying								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 33	57	3	0%	2%	9%	14%	75%	100%

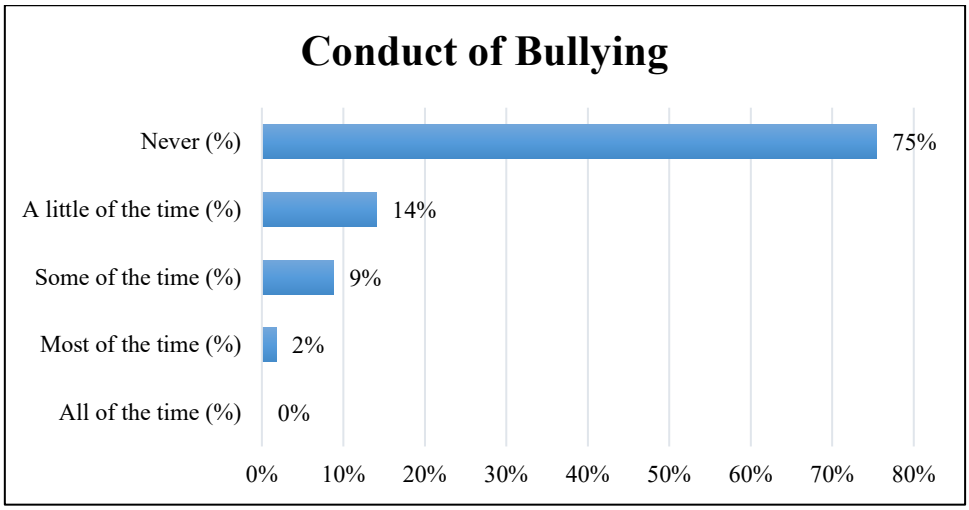


Figure 69: Conduct of Bullying

5.6.6.2 Conduct of Uploading Fake or Harmful Material

In response of two questions belonging to this category 16% children admitted of uploading, sharing or creating harmful material and 14% of children admitted to share fake news or incorrect information without authentication and involved in reposting such material without a reference. The data gathered in response of both measurement questions of this construct category is tabulated as under:

Table 5-35: Uploading Fake or Harmful Material

Uploading Fake or Harmful Material								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 34	58	2	0%	0%	3%	12%	84%	100%
Question 35	58	2	0%	0%	2%	12%	86%	100%

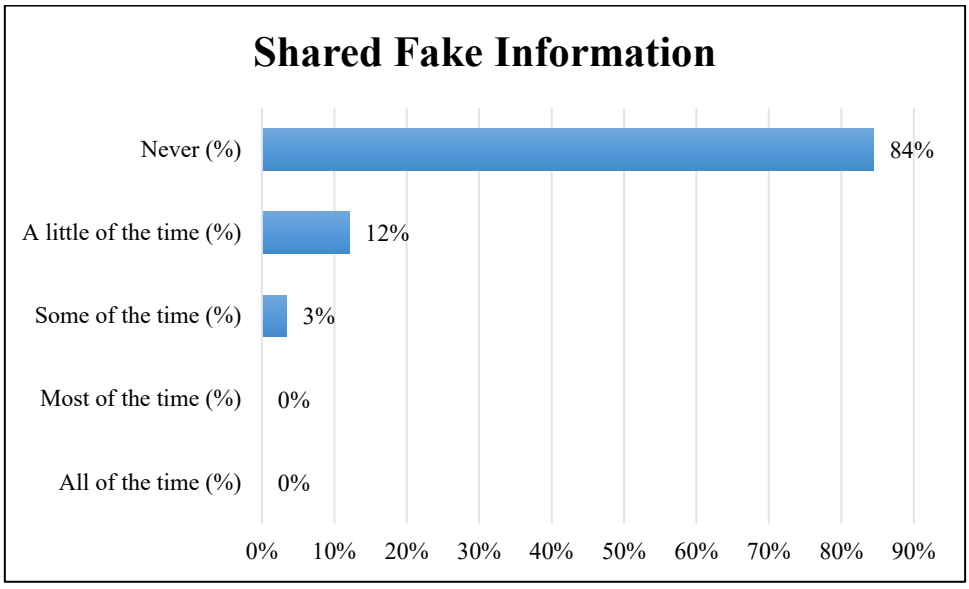


Figure 70: Sharing Fake Information

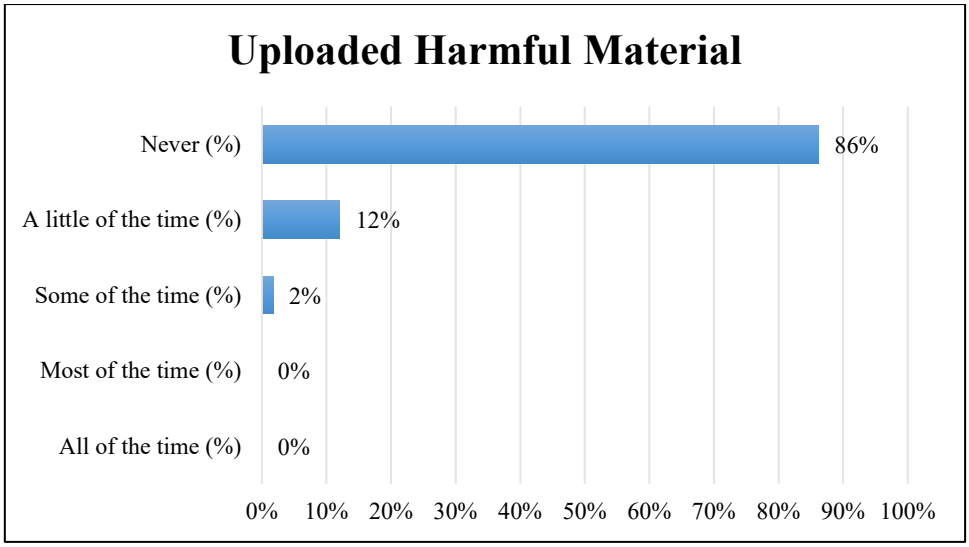


Figure 71: Uploaded Harmful Material

5.6.6.3 Privacy Risks

The privacy risks in Conduct risk category includes privacy breaching of others by your conduct i.e. by sharing screen shots etc. 16% of the targeted sample admitted to do so.

Table 5-36: Disclosing Privacy of Others

Privacy Risks								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 36	58	2	0%	3%	9%	16%	72%	100%

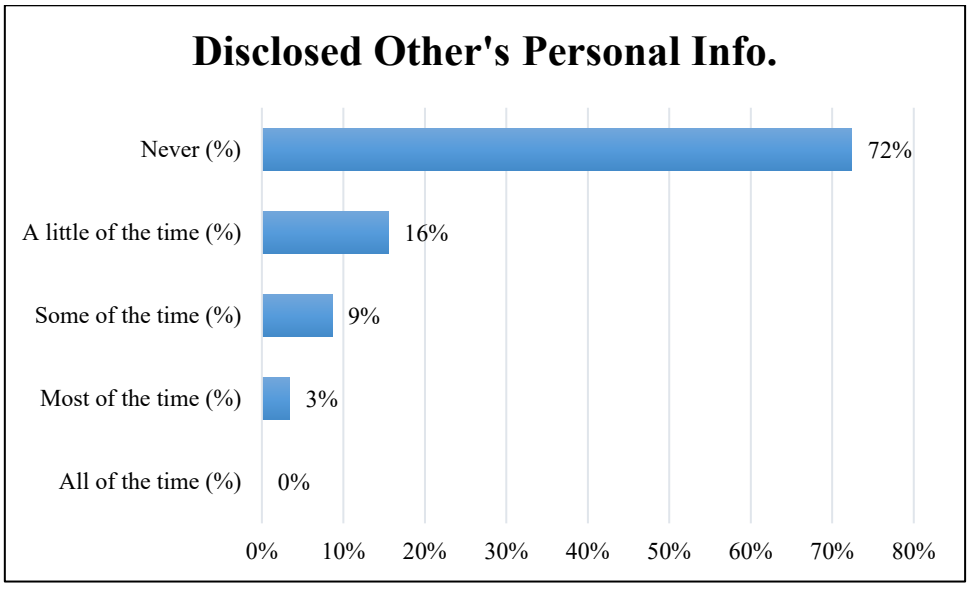


Figure 72: Disclosing Privacy of Others

5.6.6.4 Illegal Downloads

44% of children admitted to download pirated copies of books and pirated version of software and games and 14% of them committed it frequently.

Table 5-37: Illegal Downloads

Illegal Downloads								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 37	58	2	7%	7%	7%	14%	66%	100%

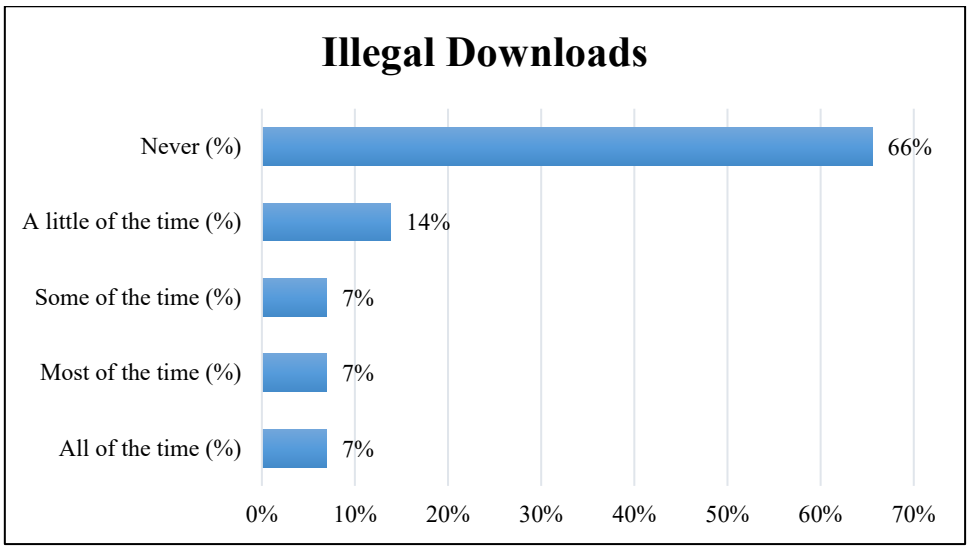


Figure 73: Illegal Downloads

5.6.7 Technological Risks

The fourth and last category of internet risks that measures risks that are not directly caused by human behaviour but by the means of technology. Results according to further categorization are as under.

5.6.7.1 Falling for Scams

Internet is full of scam offers of products and services. Children being netizens also came to face such fake deals and became a victim. 47% of the children reported for facing such scam offers and 31% of them used to see such offers with high frequency.

Table 5-38: Falling for Scams

Falling for Scams								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 38	58	2	10%	21%	5%	10%	53%	100%

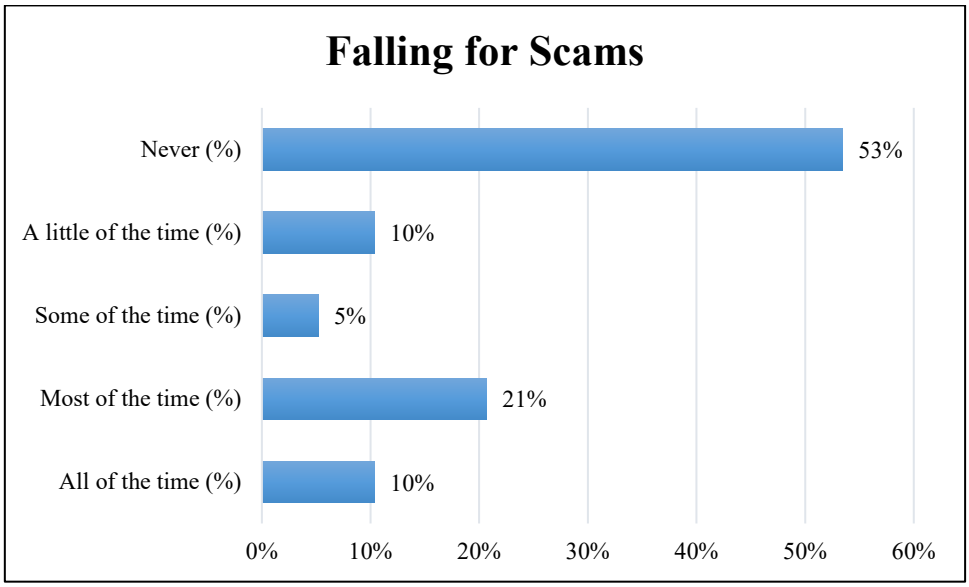


Figure 74: Falling for Scams

5.6.7.2 Accidently Downloading Malware

Accidently downloading a malware is the most common and highly occurring sub category of technological risks domain of internet risk categorization. 44% of the children told that they have accidently downloaded a malware by clicking a random pop up message or link that appear on their screens while using internet for different purposes. 50% of them have downloaded such games that are actually adware and 7% have conducted such downloads frequently. This is a very high percentage which shows that this is the most common technological risk faced by children. 26% reported data corruption due to certain game downloads. Children downloaded games that are not actually the games but malware and make them in huge trouble by corrupting all the data present on that device on which download has been done. The data is tabulated and presented below:

Table 5-39: Accidentally downloading a Malware

Accidentally Downloading a Malware								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 39	58	2	2%	5%	17%	10%	66%	100%
Question 40	58	2	2%	16%	14%	19%	50%	100%
Question 41	57	3	0%	2%	14%	11%	74%	100%

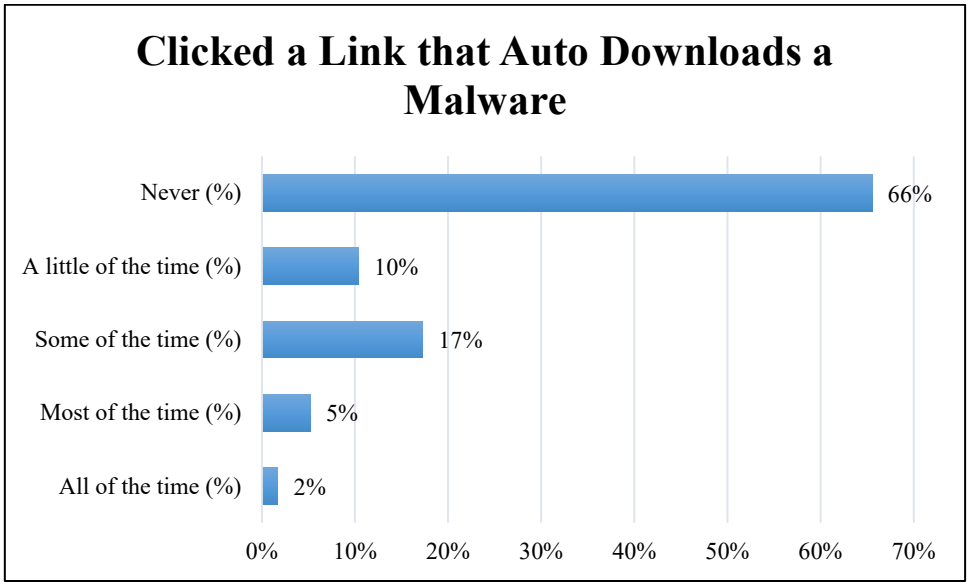


Figure 75: Auto Download of Malware

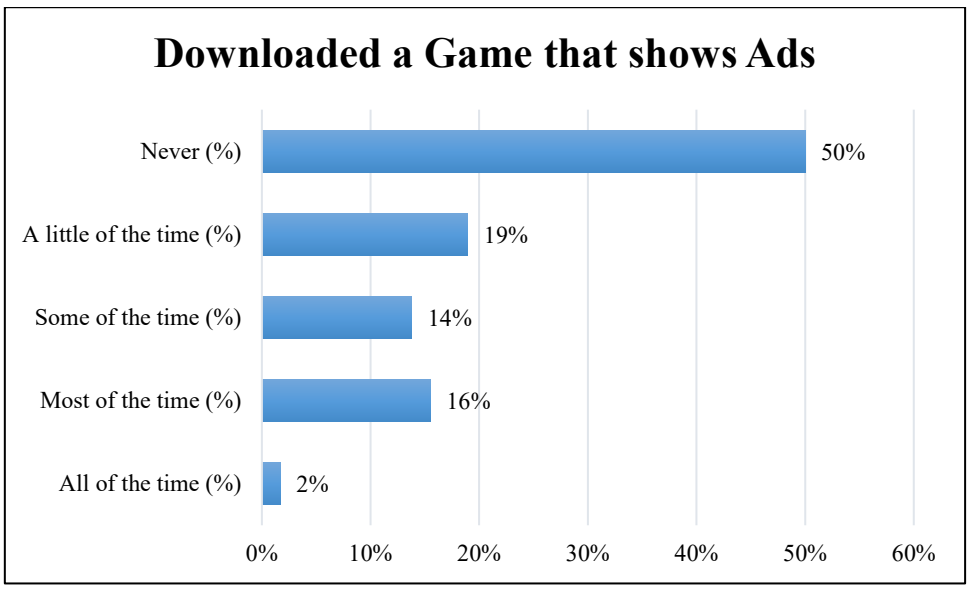


Figure 76: Games as Adware

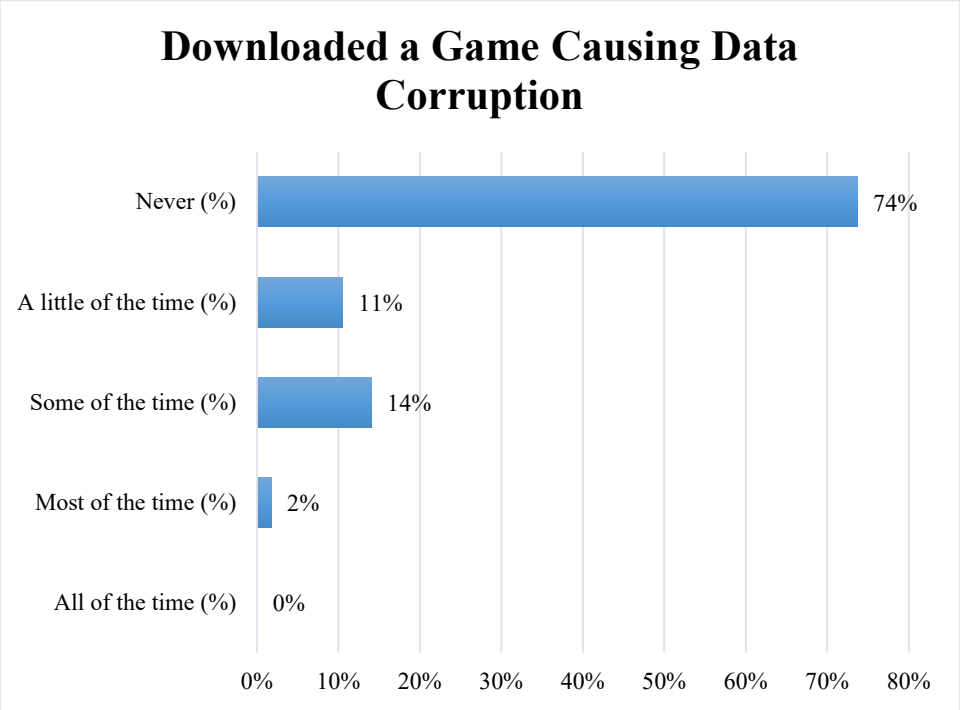


Figure 77: Game Causing Data Corruption

5.6.7.3 Phishing

This technological risk seems to be least occurring according to the results as 41% of children has experienced receiving emails that ask to click such links that consequently redirects them to malicious pages. 38% of them had received phishing emails and only 18% reported to receive such messages that include links to malicious pages.

Table 5-40: Phishing

Phishing								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 42	58	2	0%	5%	12%	9%	74%	100%
Question 43	58	2	0%	3%	7%	14%	76%	100%
Question 44	58	2	0%	0%	0%	12%	88%	100%

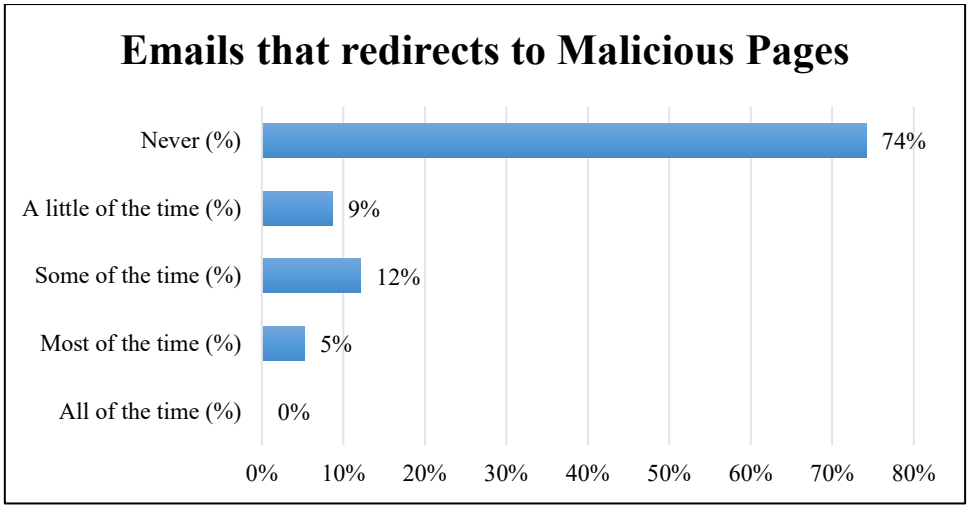


Figure 78: Email Redirecting to Malicious Pages

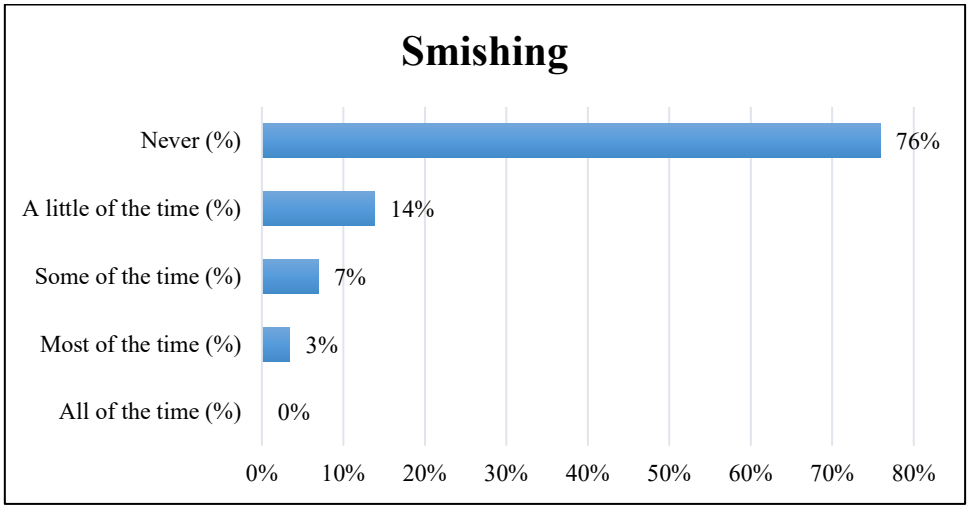


Figure 79: Smishing

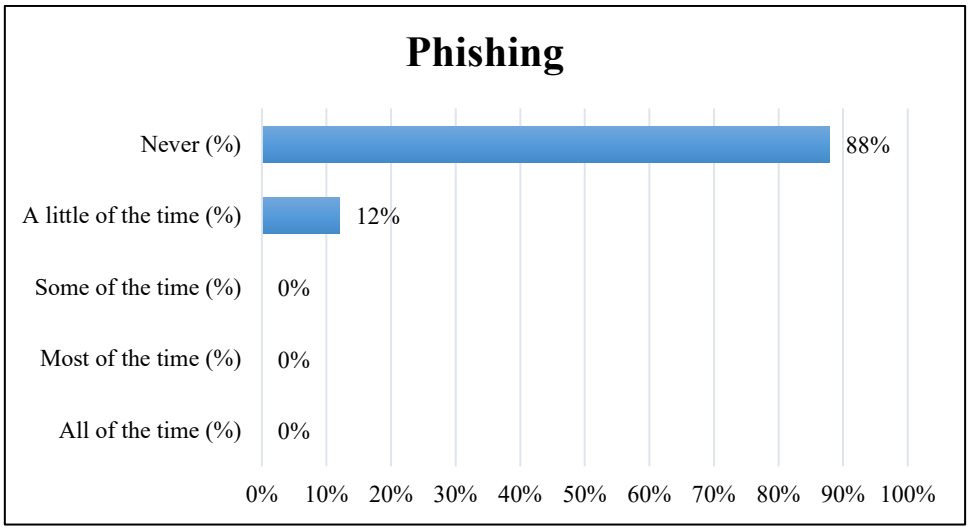


Figure 80: Phishing

5.6.8 Miscellaneous Questions

After measuring about internet risk categorization children were asked to miscellaneous questions at the end.

5.6.8.1 Most Negative Impact

The important one from them was asking about most negative impact of the internet risk situations in which 25% of the people have reported that the were disturbed most by the fake news spread on the internet. Second most reported category is Online Harassment which is one of the worst online risks. 21% of the children have reported this as having worst effects on young mind. At third place 14% of the targeted sample told that adult/violent content has most negative impact on their young minds 10% reported for both disclosure of personal data and for religious hatred and provincial bigotry. At last place 9% of the children reported bullying as the worst happening online risk to them.

Table 5-41: Most Negative Impact

Most Negative Impact										
Questions	Total Responses	Blank Answers	Bullying (%)	Harassment (%)	Violent/ Adult content (%)	Religious hatred/ Provincial bigotry (%)	Fake news (%)	Disclosure of personal data (pictures etc.)	Accidentally downloading a virus (%)	TOTAL (%)
Question 45	56	4	2%	7%	14%	23%	21%	4%	29%	100%

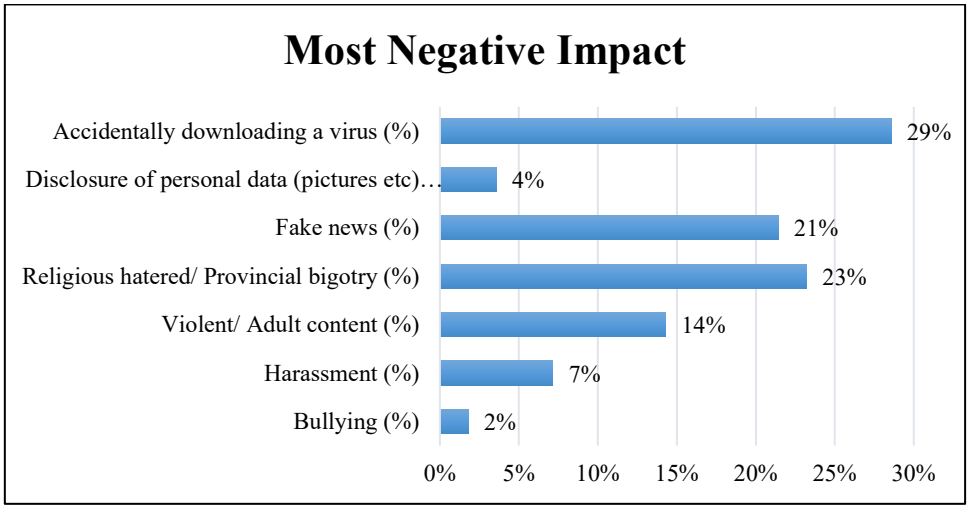


Figure 81: Most Negative Impact

5.6.8.2 Seek for Guidance

The last question of the questionnaire was intended to measure if the children have asked for proper guidance after suffering from any unwanted online risk situation or not. 72% of them had answered in agreement which is favourable condition. But still 28% of the children suffer all these undesirable situations all alone without asking for help from elders.

Table 5-42: Seek for Proper Guidance

Seek for Proper Guidance								
Questions	**TOTAL RESPONSES**	**BLANK ANSWERS**	**All of the time (%)**	**Most of the time (%)**	**Some of the time (%)**	**A little of the time (%)**	**Never (%)**	**TOTAL (%)**
Question 46	58	2	36%	7%	16%	5%	36%	100%

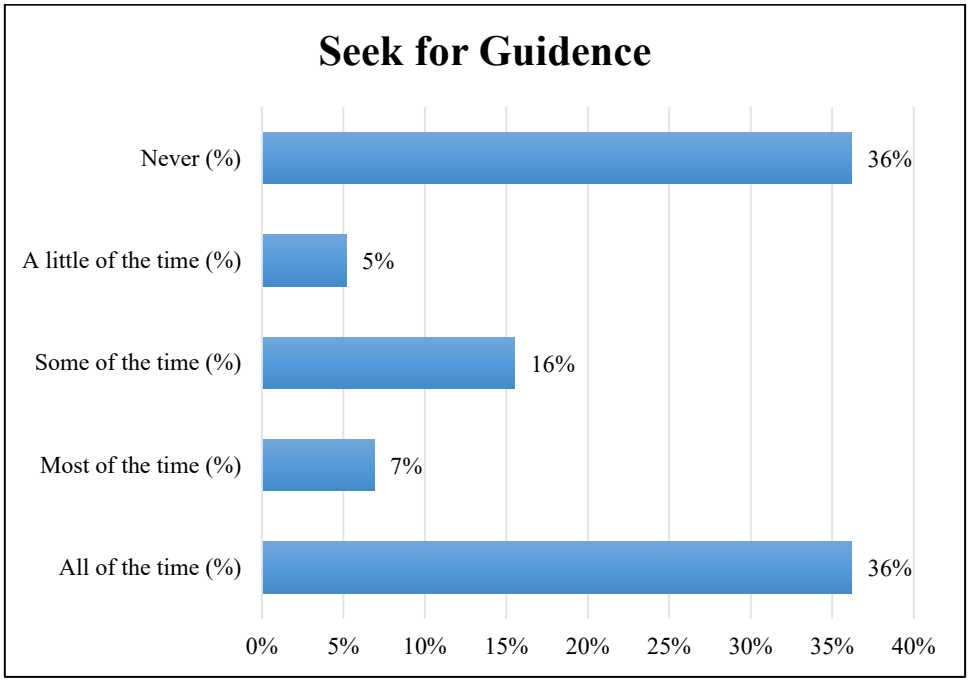


Figure 82: Seek for Proper Guidance

5.7 COMPARISON OF RESULTS GATHERED VIA ONLINE AND OFFLINE SURVEY

The survey results gathered by both the surveys are compared and summarized in the form of a table and are presented as under. This comparison is done to observe the trends in internet availability and its consequences on the further survey constructs that are aimed to be

measured. So that we better generalize the results and infer them to the whole population of Pakistan under the age of 18.

Table 5-43: Comparison of Online and Offline Survey

Constructs	Online Results	Offline Results
Internet facility	90%	66%
Webcam	34%	84%
Internet outside Homes & Schools	38%	44%
Access to Social Media	83%	28%
Personal Social Media Accounts	69%	26%
Online Time Up to 3 hours	48%	69%
Online Time 3-6 hours	22%	16%
Online Time 6-9 hours	15%	6%
Online Time 9-12 hours	5%	4%
Online Time 12+ hours	9%	6%
Activated Security Settings	69%	26%
Aware of Unsafe Internet Usage	79%	66%
Online stuff is Inerasable	49%	56%
Briefing about Online Safety	67%	88%
Adult Content	48%	24%
Violent Content	61%	63%
Drug Promotions	35%	59%
Sectarianism & Religious Hatred	52%	75%
Provincial & Linguistic Bigotry	51%	67%
Fake News	90%	86%
Altered Decision due to Online Ads	52%	44%
Purchased Online Games etc.	25%	33%
Ads leading to Inappropriate Content	55%	28%
Subscription after giving Personal Data	51%	24%
Faced Abusive Language	51%	52%
Felt Humiliation	44%	24%
Fake IDs negative messages	72%	59%

Constructs	Online Results	Offline Results
Shared Personal Info.	42%	24%
Shared Password	15%	16%
Share Photos and Events	44%	31%
Read Screen Shots of Chats	55%	45%
Filled Quizzes by giving Access to Data	34%	45%
Having Unknown Social Media Friends	39%/	21%
Met with Social Media Friends	25%/	11%
Bullied Others	13%	25%
Shared Fake Info.	19%	16%
Created Harmful Content	8%	14%
Disclosed Others Privacy	16%	28%
Downloaded Pirated Copies	42%	34%
Falling for Scam Offers	61%	47%
Clicked a Malicious Link	45%	34%
Installed Adware in form of Game	72%	50%
Installed Game Causing Data Corruption	47%	26%
Emails redirecting to Malicious Pages	41%	26%
SMSs redirecting to Malicious Pages	38%	24%
Phishing	18%	12%
Seek for Guidance	72%	64%
Male Participants	30%	29%
Female Participants	70%	71%

1. And the risk categorization on the basis of most negative impact in both surveys is as under is tabulated below. According to online survey most of the children consider fake news as most disturbing risk among all categories followed by Harassment at second place and then Violent/Adult Content, Malware, Privacy Disclosure, Religious/ Provincial Bigotry, Bullying in descending order. While in offline survey the categorization on the basis of most negative impacts on young minds is slight different. Children reported Malware as most disturbing threat and Religious/ Provincial Bigotry at second place and then Fake News, Violent/Adult Content, Harassment, Privacy Disclosure and bullying respectively.

Table 5-44: Top Internet Risk Categorization on the basis of Negative Impact

Categorization	Online	Percentage	Offline	Percentage
First	Fake News	25%	Malware	29%
Second	Harassment	21%	Religious/ Provincial Bigotry	23%
Third	Violent/Adult Content	14%	Fake News	21%
Fourth	Malware	10%	Violent/Adult Content	14%
Fifth	Privacy Disclosure	10%	Harassment	7%
Sixth	Religious/ Provincial Bigotry	10%	Privacy Disclosure	4%
Seventh	Bullying	9%	Bullying	2%

Chapter 6: CONCLUSION

6.1 ACHIEVED RESULTS:

After conduction of both online and offline surveys the data from one hundred and twenty one and eighty five respondents have been gathered respectively. After post survey adjustments of the raw data and filtering out the noise the gathered data reduced to nighty one and fifty eight respondents respectively. The data from online survey has been gathered from twenty five different cities from all the four provinces of Pakistan. The responses came from Rawalpindi, Karachi, Lahore, Quetta, Islamabad, Sargodha, Khushab, Hadali, Jauharabad, Faisalabad, Rawalakot, Lawa, Hyderabad, Gujjar Khan, Bagh, Mian Channo, Okara, Peshawar, Attock, Talagang, Bhakkar Bar, Chakwal, Pelowance, Joyia, and Multan. The respondents are between 10 to 41 years of age and are students of different schools, colleges, and universities all our country. The student participation has a diversity of different fields and educational back ground and belong to various fields of studies from primary and middle school levels to PhD students of various technical and non-technical fields as Pre-Medical, Pre-Engineering, ICS, IT, Commerce, Arts and Humanities, Information Security, Mathematics, Mass Communication, Fashion Designing, Accounts, Computer Sciences, Medical, Zoology, Software Engineering, Banking and Finance, Urdu and Economics. This data after adjustments have filtered out the respondents greater than the age of 18 as the target audience of the study are children. The offline survey has been conducted in a few public sector institution of Federal Area of Islamabad. In both the surveys two third participation is from the female students i.e. 71% and 69% and one third is from the boys which is 29% and 31% respectively.

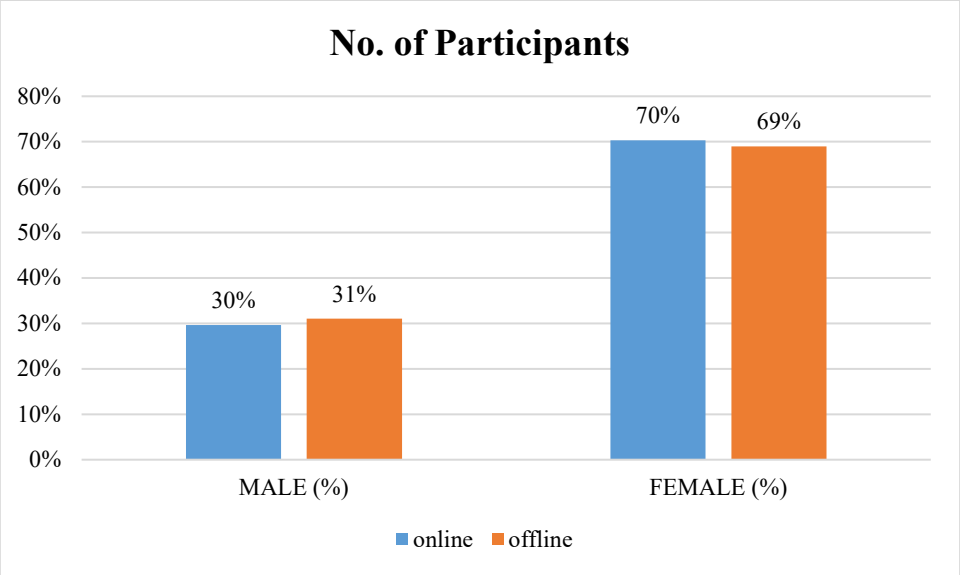


Figure 83: Gender wise Participation of Respondents

6.2 SIGNIFICANT FINDINGS:

The results and discussion in previous chapter shows that the ratio of participation of students on the basis of gender is almost same. The results gathered via online survey are more general, reliable and can be inferred to the whole target population due to diversity of different educational and residential backgrounds in it as compared to the offline conducted survey which is limited to a public sector institution in federal area of Islamabad.

Categorization of most damaging risk on the basis of findings is as follows. 25% of the people have reported that they were disturbed most by the fake news spread on the internet. Second most reported category is Online Harassment which is one of the worst online risks. 21% of the children have reported this as having worst effects on young mind. At third place 14% of the targeted sample told that adult/violent content has most negative impact on their young minds 10% reported for both disclosure of personal data and for religious hatred and provincial bigotry. At last place 9% of the children reported bullying as the worst happening online risk to them. On the other hand the categorization is quite different in offline survey results. Children reported Malware as most disturbing threat (29%) and Religious/ Provincial Bigotry (23%) at second place and then Fake News (21%), Violent/Adult Content (14%), Harassment (7%), Privacy Disclosure (4%) and bullying (7%).

6.3 LIMITATION OF STUDY

The offline survey was unable to studied on larger scale due to lack of interest of the managers of educational sectors in research studies having more focus on grade base result system. As many of the public and private sector platforms have been contacted but they denied to being part of the study.

6.4 IMPROVISING CYBER SECURITY AWARENESS

For offline respondents awareness sessions having highlights about internet risks and tips and guidelines have been shared for using cyber space wisely to remain safe online and for online respondents a tri fold brochure having possible risks and internet safety tips have been shared. The designed brochure is also attached in Appendix B. The communicated safety guide lines are as under:

6.4.1 Content Risk Mitigation Techniques

6.4.1.1 Provocative Content

This type of content can only be avoided by parental control. Different video playing websites and other internet platforms suggest such type of content at random. And these type of content

usually gone viral and children randomly face this. To avoid such suffering parents must be aware and on children mode on their internet devices and use parental control passwords provided by different apps. Parents must allow their children to use internet in shared places

6.4.1.2 Incorrect False Information

Children must not believe everything they read or see online. Many hostile elements spread rumors and bigotry to create depravity in the nation.

6.4.1.3 Commercial Content

This can also only be controlled by parental awareness and supervision. Financial apps must be used in child restricted mode. Some of the recent and useful apps for parental control are reviewed and summarized in the form of a table in Table 6-1 [32]. Top five best apps are reviewed and the analysis is on the basis of cost, effectiveness, No. of users etc. This fact should be kept in mind that the technology is gaining advancements day by day. And the apps that are worth to use at present day may not be worthy in future. Hence parents should stay connected and updated to latest technology for better surveillance. The review is as under:

Table 6-1: Best Parental Control Apps Review

Application Name	Social Media Surveillance	Email Surveillance	GPS Monitoring	Remote Session End	Distinguished Characteristic
Bark	Available	Available	Not Available	Available	Overall Best App
Boomerang	Not Available	Not Available	Available	Available	Best for Young Children
Kaspersky	Available	Not Available	Available	Not Available	Budget Friendly
Family Time	Not Available	Not Available	Available	Available	Best for IOS Devices
Qustodio	Available	Not Available	Available	Not Available	Best Reporting Dashboard

6.4.2 Contact Risk Mitigation Techniques

6.4.2.1 Online Risks

This kind of risks such as cyber bullying, exploitation and privacy risks can be avoided by following under described tips:

1. Always report elders when you face a mean communication or disturbing comment
2. Never share your personal information online with anyone specifically with someone unknown
3. Use strong passwords created with combination of characters, numbers and special characters like p@s$w0rd, I2E4
4. Use password which are not easy to guess like 0r@n9ed0gf1uffy$kin

6.4.2.2 Offline Risks

Never meet with someone you met online as they are still strangers. If do so, meet in presence of your parents and with their proper permission.

6.4.3 Conduct Risk Mitigation Techniques

1. Do not bully or harass others
2. Do not create/ share information which seems incorrect or false. It is advisable to first consult your parent if anything looks suspicious
3. Never disclose others personal chat or information
4. Do not install games or apps without knowledge/permissions of your parents or guardian.
5. Do not click random links. These are the largest source of data breach.

6.5 GENERAL RECOMMENDATIONS

On average more than fifty percent of the targeted population have suffered from different types of online risks. In some severe cases this percentage increases to seventy five to eighty percent. To reduce these sufferings following steps should be taken.

1. The steps should be taken on state level to mitigate the online sufferings of young children.
2. An effective curriculum should be designed for ICT having more emphasize on Cyber Security.
3. A same kind of research should be done to explore the awareness level of teachers and parents to gauge the shortcomings.
4. Awareness campaigns should be conducted for parents and teachers so that they can be able to better trained their children and students to remain safe online.

5. Awareness campaign should be conducted for students as well on national level.

6.6 FUTURE WORK

This domain need a lot of study to be done to make the nation cyber wise. For this purpose following are some proposed topics that should be studied in future

1. Same kind of study should be done for teachers and parents as well on national level to improvise cyber security awareness in them consequently awareness in children will also increase
2. Awareness level of 18+ younger populations must also be studied as they use internet more frequently
3. Comparison of urban and rural areas & public and private sectors of education should be done in future.

References

[1] R. v. S. Mariska de Lange, "An e-Safety Educational Framework in South Africa," 2012.

[2] B. A. I. R. A. W. Muhammad Tariq, "Cyber Threats and Incident Response Capability-A Case Study of Pakistan," in *2013 2nd National Conference on Information Assurance (NCIA)*, Islamabad, 2013.

[3] A. A. K. M. Y. Rubab Syed, "Cyber Security: Where Does Pakistan Stand?," SDPI, Islamabad, Pakistan, February 2019.

[4] S. M. S. M. K. T. P. N. H. A. Jawad hussain Awan, "CYBER THREATS/ATTACKS AND A DEFENSIVE MODEL TO MITIGATE CYBER ACTIVITIES," *Mehran University Research Journal of Engineering and Technology,* p. 8, 2017.

[5] Sonia Livingstone, "Online Freedom and Safety for Children," Stationary Office Limited, November, 2001.

[6] Clara Brady, "Security Awareness for Children," London, 2010.

[7] US Department of Education, "Cybersecurity: 7 Ways to Keep Kids Safe Online," 2015.

[8] B. D. W. H. V. K. T. S. M. Valcke, "Long-Term Study of Safe Internet Use of Young Children," *Computer and Education,* pp. 1292-1305, 14 Jan, 2011.

[9] J. R. Nigel Martin, "Children's cyber-safety and protection in Australia: An analysis of community stakeholder views," *Crime Prevention and Community Safety,* pp. 165-181, 2012.

[10] Unicef, "Child Online Protection in India," National Commission for Protection of Child Rights, 2016.

[11] UNDP Pakistan, "UNLEASHING THE POTENTIAL OF A YOUNG PAKISTAN," 2017.

[12] S. F. A. P. Shirley Atkinson, "Securing the next generation: enhancing e-safety awareness among young people," *Computer Fraud & Security,* pp. 13-19, 2009.

[13] M. A. Abbasi, "outline of Program Prism and its Effects on Cyber Security of Pakistan," *International Journal of Research in IT, Management and Engineering,* p. 6, 2016.

[14] Kaspersky Lab, "Kaspersky Lab Study: Children Online," Kaspersky Lab, March, 2015.

[15] The News International, "Online Violence Against Children on Rise in Pakistan: Unicef," Islamabad, Feb 06, 2019.

[16] Muhammad Farooq, "Stop Cyber Bullying," Dawn, March 06, 2016.

[17] A. Tsirtsis, N. Tsapatsoulis and M. Stamatelatos, "Cyber Security Risks for Minors: A Taxonomy and a Software Architecture," in *11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, Cyprus, 2016.

[18] P. Tasevski, "Information & Security," *IT AND CYBER SECURITY AWARENESS-RAISING CAMPAIGNS,* vol. 34, no. 1, pp. 7-22, 2016.

[19] M. Bada, A. . M. Sasse and J. . R. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," *International Conference on Cyber Security for Sustainable Society, 2015,* 9 January 2019.

[20] Z. Dlamini and M. Modise, "Cyber security awareness initiatives in South Africa: a synergy approach," in *7th International Conference on Information Warfare and Security*, University of Washington, Seattle, USA, 2012.

[21] N. Kortjan and R. . v. Solms, "A conceptual framework for cyber-security awareness and education in SA," *South African Computer Journal 52,* 2014.

[22] G. . C. Zilka, "AWARENESS OF ESAFETY AND POTENTIAL ONLINE DANGERS AMONG CHILDREN AND TEENAGERS," *Journal of Information Technology Education : Research,* vol. 16, 2017.

[23] M. B. a. J. R. N. Elmarie Kritzinger, "A study into the cyber security awareness initiatives for school learners in South Africa and the UK," in *10th World Conference on Information Security Education (WISE-2017)*, School of Computing, University of South Africa, Global Cyber Security Capacity Centre, University of Oxford, Department of Computer Science, University of Oxford, 2017.

[24] H. A. Q. J. B. I. Saeed S. Basamh, "An Overview on Cyber Security Awareness in Muslim Countries," *International Journal of Information and Communication Technology Research,* vol. 4, 1 January 2014.

[25] F. S. M. A. J. N. F. M. S. A. M. S. R. S. Iskandar Ishak, "A Survey on Security Awareness among Social Networking Users in Malaysia," *Australian Journal of Basic and Applied Sciences,* vol. 6(12), pp. 23-29, 2012.

[26] *Cyber Safety for School Children, A Case Study in the Nelson Mandela Metropolis,* 2013.

[27] B. Gawronski, *ATTITUDES CAN BE MEASURED!,* 5 ed., vol. 25, Social Cognition, 2007, pp. 573-581.

[28] E. D. d. Leeuw, "To Mix or Not to Mix Data Collection Modes in Surveys," *Journal of Official Statistics,* vol. 21, pp. 233-255, 2005.

[29] J. DAIKELER, . M. BOSNJAK and K. LOZAR MANFREDA, "WEB VERSUS OTHER SURVEY MODES: AN UPDATED AND EXTENDED META-ANALYSIS COMPARING RESPONSE RATES," *Journal of Survey Statistics and Methodology,* vol. 8, pp. 513-539, 2020.

[30] R. E. Petty and J. T. Cacioppo, "Issue Involvement As a Moderator of the Effects on Attitude of Advertising Content and Context," *Advances in Consumer Research ,* vol. 8, 1981.

[31] P. P. BIEMER, "TOTAL SURVEY ERROR : DESIGN, IMPLEMENTATION, AND EVALUATION," *Public Opinion Quarterly,* vol. 74, no. 5, p. 817–848, 2010.

[32] C. Habas, "safewise," 21 September 2021. [Online]. Available: https://www.safewise.com/resources/parental-control-filters-buyers-guide.

[33] I. Ishak, F. Sidi, M. A. Jabar , N. F. M. Sani, A. Mustapha and S. R. Supian, "A Survey on Security Awareness among Social Networking Users in Malaysia," *Australian Journal of Basic and Applied Sciences,,* vol. 6, no. 12, pp. 23-29, 2012.

[34] S. M. Jawad Awan, "Threats of Cyber Security and Challenges for Pakistan," Jamshoro, Sindh, 2016.

[35] A. M. Narmeen Shafqat, "Comparative Analysis of Various National Cyber Security Strategies," *International Journal of Computer Science and Information Security,* vol. 14, no. `1, p. 8, January 2016.

[36] S. M. M. H. S. F. H. S. Jawad Hussain Awan, "Security of Egovernment Services and Challenges in Pakistan," in *SAI Computing Conference*, London, UK, 2016.

[37] C. Brady, "Security Awareness for Children," London, 2010.

Appendix A

Questionnaire for exploring Cyber Security Awareness in Young Pakistani Children (10-18 years)

This survey is being done for research purpose as a requirement of MS degree. The questionnaire is aimed to explore the awareness of young Pakistani generation (from 10 to 18 years of age) about the threats hiding on internet. Your participation is highly appreciated and acknowledged. Please contribute to play your positive role as a sensible citizen.

Your Name:	
Age:	
Class:	
Gender:	◯ **Male** ◯ **Female**
Field of Study:	
School/ Institute:	
City:	

What was your favorite online activity before COVID-19?

	1	2	3	4	5	6	None
Entertainment (Cartoon/ Movies/ Songs etc.)							
Social Media (Facebook/WhatsApp/Instagram etc)							
Online Gaming							
Online Study							
Online Shopping							
Other							

What is your Favourite online activity after COVID-19?

	1	2	3	4	5	6	None
Entertainment (Cartoon/ Movies/ Songs etc.)							
Social Media (Facebook/WhatsApp/Instagram etc)							
Online Gaming							
Online Study							
Online Shopping							
Other							

Have you ever used webcam?			◯ **Yes**	◯ **No**
How much time in hours you spend daily on internet?				
◯ **Up to 3 hours**	◯ **3 to 6 hours**	◯ **6 to 9 hours**	◯ **9 to 12 hours**	◯ **More than 12 hrs**
Do you have access to any computer, mobile or tablet with internet facility?			◯ **Yes**	◯ **No**
Do you have any access to internet other than home and school computers?			◯ **Yes**	◯ **No**
Do you have access to social media accounts?			◯ **Yes**	◯ **No**
Do you have access to social media accounts?			◯ **Yes**	◯ **No**
Have you activated security settings on your social media accounts?			◯ **Yes**	◯ **No**
Are you aware of harms/ threats of unsafe internet usage?			◯ **Yes**	◯ **No**
Do you know once you posted something online can never be erased?			◯ **Yes**	◯ **No**
Have someone (parents or teachers) ever briefed you about online safety?			◯ **Yes**	◯ **No**

Have you ever seen age inappropriate/ adult (فحش/بےہودہ) content online?				
◯	◯	◯	◯	◯
Have you ever seen violent (پر تشدد) content online?				
◯	◯	◯	◯	◯
Have you ever seen drug (نشہ آور) promoting content online?				
◯	◯	◯	◯	◯
Have you ever seen such posts/ videos that promote sectarianism (فرقہ واریت) and religious hatered (مذہبی منافرت)?				
◯	◯	◯	◯	◯

Have you ever seen such posts/ videos that promote provincial bigotry (صوبائی تعصب)?				
Have you ever seen fake news or false information online?				
Have you ever changed your decision due to online advertisement?				
Have you ever purchased online games or ringtones etc?				
Have you ever seen advertisements that lead you to inappropriate content?				
Have you ever subscribed/ logged in after giving your personal information?				
Have you ever faced abusive (گالی) or unethical (غیر اخلاقی) languages on social media or other online platforms?				
Have you ever feel insulted online?				
Have you ever noticed identity theft (جھوٹی شناخت) or fake profiles online?				
Have you ever faced online harassment/ exploitation?				
Have you ever shared your personal information or data online?				
Have you ever shared your password with someone online?				
Do you regularly share your daily routine (e.g. your family photos & social events) on social media?				
Have you ever read screen shots of personal chats of others?				
Have you ever filled some type of psychological or educational quiz that asks access to yours or your friends' personal data?				
Do you have such friends on social media who are unknown to you in real life?				
Have you ever met someone in real world after you have first met on social media?				
Have you ever bullied others online?				
Have you ever shared incorrect or fake information online?				
Have you ever created or uploaded harmful material online?				
Have you ever disclosed other's personal data through screen shots etc.?				
Have you ever downloaded pirated versions of games or books etc.?				
Have you ever seen such offers as free access to online games etc.?				
Have you ever clicked on a link that automatically download a malware/ virus that troubles you later on?				
Have you ever downloaded a game that shows a lot of advertisement?				

Have you ever downloaded a game that causes data corruption or virus etc. ?				
⬭	⬭	⬭	⬭	⬭
Have you ever got such emails that ask you to click on links that redirect you to malicious pages?				
⬭	⬭	⬭	⬭	⬭
Have you ever got such SMSs that ask you to click on links that redirect you to malicious pages?				
⬭	⬭	⬭	⬭	⬭
Have you ever got an email from a family member or friend that was not actually sent by them?				
⬭	⬭	⬭	⬭	⬭
Which situation put most negative impact on your mind?				
⬭ Bullying	⬭ Harassment	⬭ Violent/ Adult Content	⬭ Accidently downloading a virus	
⬭ Religious hatred/ Provincial bigotry	⬭	⬭ Disclosure of personal data (pictures etc.)		
Have you ever informed anyone (parents or siblings or teachers) for proper guidance?				
⬭	⬭	⬭	⬭	⬭

Appendix B

BE CYBER SMART

S **SAFE**: Stay safe by not posting your personal info. Including passwords, email IDs, Home addresses etc.

M **Meeting UP**: Never meet up with persons you know online, they are still strangers, if do so, first ask your parents

A **Accepting Stuff**: Do not accept files from unknown IDs and Do not Accept friend Request of unknown Persons

R **Reliability Check**: Before opening any email or clicking any link or pop-up, first check the source is reliable or not

T **Tell Elders**: In case of any unwanted situation e.g. receiving strange or mean comments tell elders for Help

You can lodge a complaint to CCW- FIA, by calling at Helpline No. **9911** or file an online complaint through email at **helpdesk@nr3c.gov.pk**. Alternatively you can call at any of the following Cyber Crime Reporting Centers.

Cyber Crime Reporting Centers	Phone Numbers
Islamabad (ICT)	051-9262106, 051-9262107-08
Rawalpindi	051-9330717 051-9334919 051-9330720
Lahore	042-99332744
Peshawar	091-9217109
Quetta	081-2870057
Karachi	021-99333950
Multan	061-9330999
Sukhar	071-9310849
Faisalabad	041-9330865
Gujranwala	055-9330015-16
DI Khan	0966-852945
Hyderabad	022-9250009
Gwadar	0322-2451500
Gilgit	05811-920409
Abbottabad	099-2384148

BE CYBER SAFE

A GUIDE FOR CHILDREN TO IDENTIFY POSSIBLE RISK AND GUIDELINES TO EXPLORE THE INTERNET SAFELY

By Rabia Kalsoom

MS System Engineering-04

MCS-NUST

Internet gave rise to opportunities as well as threats. To remain safe online don't stop using internet, just be aware of possible risks and follow safety guidelines

POSSIBLE RISKS

Sharing your personal information like address, phone number, password etc. online.

Using simple and easy passwords like 1234, mypetdog.

Installing virus through games and apps.

Clicking random links while browsing especially those offering free offers.

Creating/ uploading incorrect or harmful material.

Falling prey to incorrect information.

Accepting friend requests of strangers.

Meeting up with online friends

Free internet Services at public places

Scam offers/Illegal Downloads

SAFETY GUIDELINES

Do not share your personal information online with anyone specifically with someone unknown.

Use strong passwords created with combination of characters, numbers and special characters like p@s$w0rd, I2E4

Use password which are not easy to guess like 0r@n9ed0gf1uffy$kin.

Do not install games or apps without knowledge/permissions of your parents or guardian.

Do not click random links. These are the largest source of data breach.

Do not create/ share information which seems incorrect or false. It is advisable to first consult your parent if anything looks suspicious.

Do not believe everything you read or see online. Many hostile elements spread rumors and bigotry to create depravity in the nation.

SAFETY GUIDELINES

Don't accept friend requests from strangers

In case of facing bullying or harassment always ask for help from elders, Never stay Quiet

Never meet up with online friends, they are still strangers

Never connect to free Wi-Fi available at public places as they are not safe

Never click on free offers such as games etc. these are scams

Never download pirated versions of games, software, books etc. as it's illegal

In case of any unwanted situation or bad suffering you can file a complaint to FIA

BE CYBER SMART

BE CYBER SAFE