CYBER SECURITY SENSITIZATION: A CASE STUDY OF ADOLESCENTS IN PAKISTAN

By

Syed Usman Ali Shah

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 Information Security

Aug. 2017

ABSTRACT

As a human, we have been confronting with risks throughout our whole lives. The advent of internet has introduced a new set of risks that is risks in digital world. This new aspect brought forward a widespread debate and discussion especially risks for adolescents (aged 12-18 years). Parents are found confident enough to teach their children about risks in other aspects of life but they extremely lack in guiding them about safety in the cyber space. This could be because of the digital generational gap that is present between parents and kids. Parents believe the nonexistence of certain knowledge and skills about this novel technology and as a result of this causes role reversal whereas kids are much better users of information and communications technology (ICT).

Although adolescents are tech-savvy and possess the ability to use information and communications technology for useful purposes, yet they are unfamiliar with the risks and threats in this digital era. The terms “Cyber-ethics”, “Cyber safety” and “Cyber security” are unfamiliar to them, known as C3 framework for promoting responsible use [1]. In the past, efforts were made in providing young people security through access controls but this causes an obstacle in their way of opportunities. A new approach to allow them taking full benefits from this digital world enforces a strong recommendation to provide them with respective knowledge and skills which will make them understand the risks and threats associated with their use and the countermeasures and safety precautions to guard them. Therefore, a very important step is to raise their awareness about the security and safety issues and increase their ability to defend themselves against potentially harmful actions. A responsible and appropriate use while accessing, using, collaborating and creating technology will help them enter the doctrine of “Digital citizenship”, also known as digital wellness or digital ethics; a concept by International Society for Technology in Education. [2]

One of the key defenses to address adolescent’s need is the introduction of a cyber security awareness program. These programs make sure that young people have the right tools in place and adopt appropriate behaviors that can protect them. The purpose of this study is to evaluate the present assessments on the threats and issues and identify different kinds of risk children face on the internet around the world comparing various cyber security awareness programmes and respective material resources. The second

stage consist of a survey about need assessment to assess the level of usage and online activities as well as security awareness level among Pakistani secondary school students. Based on the findings of that survey, cyber risks to adolescents in Pakistan will be identified. At last, cyber security awareness programme specific to adolescents will be designed and developed considering various methodologies and approaches already developed that will be publicly available to be incorporated in the educational curriculum. By adopting such a programme, the author believes that we can permit our children to take full advantages and opportunities of the internet and enjoy a safer online experience.

ACKNOWLEDGMENTS

I would first like to thank my thesis advisor Dr Baber Aslam, PhD of the Military College of Signals/Information Security department at National University of Science and Technology (NUST). He constantly allowed this paper to be my own work, but directed me in the right direction whenever he believed I needed it.

Also, I would be pleased to thank the other thesis committee members: Dr Imran Rashid, PhD and Asst. Prof. Mian Muhammad Waseem Iqbal, for their inspiration, insightful remarks, and solid questions.

I also thank my fellow classmates in Military College of Signals: Hassan Ishfaq, Muhammad Haseeb Jalalzai, Asad Malik, Naveed Ashraf Chattha and Irfan Afzal Butt for the stimulating discussions, for the long lasting work together before deadlines, and for all the fun we have had during our time at MCS.

At last, I would like to thank my family: my parents Syed Mahram Shah and Tahira Jabeen, for giving birth to me at the first place and supporting me in all aspects throughout my life. My wife Sadaf Usman, for believing in me and supporting me all the time.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

1.1 Background

Information and communications technologies (ICT) have become an indispensable part of lives of our children. They offer an extensive series of opportunities as educational and communication tools. They are a vital source of information and motivate imagination and efficiency. Unfortunately, internet usage has undesirable consequences: threats come across all the time. Those threats include but not limited to unrestricted access to unsuitable material, unwanted interaction with outsiders, and harassment. Kids do not possess the required skill or expertise to handle those threats. This arises the question about what should be done to make them able to protect themselves from these online risks.

Removing online risks is a very difficult job. In the past, risks to children have been tried to be reduced by limiting their access. Age confirmation tools, parental monitoring and administration and social networking sites for children-only are few ways to achieve this. Nevertheless, study has shown [3] that children can avoid these controls. Also, it restricts their chances of exploration and still leaves children exposed to risks whom parents do not know about these controls. A highly effectual solution is required. We can vest the kids with the essential expertise and knowledge they require to remain protected online [4]. We can build awareness of the threats they encounter and teach them the right protective and safety measures they can adopt.

A cyber security awareness program designed specifically for adolescents (aged 12-18 years) can accomplish the purpose. It will inspire kids to adopt considerable measures for safe surfing on internet and will encourage them to promote good safety practices. Its goal will be to make kids not only attentive to the risks they face, but also educate them about the safety precautions they can utilize to defend themselves.

1.2 Problem Statement

From the literature, the researchers found that secondary school students are considered as a high security risk and attractive candidates for security attacks [5], and there is a

tangible need of highly concern in this age to make the responsibility of security awareness grows with the user behavior. Therefore; the age of adolescence (12-18) can be the ideal period to fulfil this challenge. In developmental psychology, adolescence is viewed as a transitional period between childhood and adulthood, whose cultural purpose is the preparation of children for adult roles. The research question is:

"Being the weakest factor in security posture, how to raise security awareness level of adolescents (aged 12-18 years) in Pakistan to help them become safer, wiser and responsible digital citizens."

This study considers the necessity for a Cyber Security Awareness programme for adolescents (aged 12-18 years). It detects the types of risk kids face on the internet, examines the outcomes of a survey considering kid's activities online and outlines the objectives of a cyber security awareness programme for adolescents. By adopting such a programme, the author believes that we can permit our children to earn complete benefits from the Internet and experience a safer online practice.

1.3 Research Objectives

This study delivers solution to the abovementioned problem by offering cyber security awareness program for adolescents. The objectives that this study lays down to accomplish are:

a. Reviewing the level of research already carried out in the field and comparing international cyber security awareness program resources.
b. Reviewing all the governmental and non-governmental guidelines, practices and legislations for cyber security awareness program development.
c. Reviewing the work already done in this domain in Pakistan, identifying the cyber risks for adolescents with specific reference to Pakistan.
d. Researching the level of usage and awareness of adolescents (aged 12-18 years) in Pakistan via questionnaire and direct interaction to better understand their safety needs.
e. Developing suitable awareness material through localization of existing content geared to the Pakistani audience.

1.4 Scope of Study

The study applies to Secondary School (SSC) and Higher Secondary School (HSSC) students aged between 12 to 18 years in Pakistan. The research also encompasses parents and teachers of those students to access the level of knowledge they possess and to guide them comprehensively the role they must play to contribute in this awareness program.

1.5 Significance of Research

As per UNICEF [6], Pakistan has 35 per cent of the population aged 18 or under which makes it one of the largest youth bulges in the world. Although the kids incorporated in this figure are much younger to understand cyber security concerns yet they are the potential largest users of this digital world. No research has been made to assess the level of awareness this target group possesses and what they need to know, neither any awareness material is available to be used to educate those masses about cyber security.

1.6 Research Methodology

1.6.1 Literature review

A literature review was steered to accumulate all the applicable research on the subject to date. This was examined to determine the hitches and problems that have been raised about the adolescents and the Cyber World. The author chose two studies to focus on; A thesis paper submitted to the university of London titled *Security awareness for children* [7] and The *EU Kids Online - Findings. methods. recommendations Study* [3]. The former paper was preferred because the target audience was almost the same to the author's selected target audience and the latter as it reveals numerous noteworthy deviations in children's usage of the Internet.

The target audience for the survey was selected by a statistical procedure known as simple random sampling. The age range of the target audience is twelve to eighteen (12-18) years. No research has been made exclusively on this age group to date. The author circulated self-administered need assessment survey questionnaire to all four categories of primary and secondary schools i.e. public, private (local), private (international) and military schools. Afterwards, interviews of half of the respondents were conducted to verify the response and results.

1.6.2 Surveys

Surveys have been conducted for the following three target audiences:

a. Adolescents (aged 12-18 years)
b. Parents
c. Teachers

Three different surveys were conducted for different target audience; primary school students aged between 12 and 18, parents of these students and their teachers. This survey finalized by 405 Pakistani children, parents and teachers intended to fold evidence on these kids' internet conducts; regularity of access, activities on the internet, awareness about the risk factors and their knowledge of the security measures. Parents were measured to build an overall understanding of their parenting attitudes and conducts concerning their kids' internet access and to find the level of their awareness of few technical security measures. A third survey was conducted to gain information regarding teacher's interaction of the internet with adolescents and to determine their knowledge of current children internet safety initiatives.

1.6.3 Survey analysis

The survey for adolescents has focused on three broad risk factors; Contact, Conduct and Content. These will be explained later. Mostly, a three-point scale has been used to assess the level of awareness about different risks and safety measures i.e. Yes, No and Do Not Know. The collective response indicates the overall usage and access level of children to internet and internet devices along with the level of knowledge and awareness they possess about the risks they normally face.

The results of the survey have been input in a statistical analytics software i.e. SPSS [8] to analyze the usage level and level of awareness as a whole. SPSS provides descriptive statistical analysis and reporting of survey data including cross tabulation, frequencies and descriptive.

1.7 Author's contribution

The conducted survey lead to a gap analysis between the current level of cyber security awareness of the adolescents and the required level of awareness suggested by different cyber security awareness programs of different organizations around the globe. A comparative analysis of many cyber security awareness programs for children has been

also made to review the existing research on the issues and dangers children face on the internet. Based on the findings of the survey, cyber security awareness programme has been designed and developed through localization of existing content geared to the Pakistani audience that will be publicly available to be incorporated in the educational curriculum.

1.8 Thesis Outline

The first chapter of the thesis discusses the introduction including the background of the topic, problem statement, scope, significance, methodology and the author's contribution. Chapter 2 comprises of literature review which highlights the present state of cyber security laws and regulations in Pakistan, the importance of higher awareness level among adolescents as per compliance requirements by different standards and frameworks and at last compares most significant and result oriented cyber security programs around the world. Chapter 3 discusses adolescents' online activities and nature of internet usage. Using the said data and results of the survey, the author identifies different risks to children on the internet according to their activities and interests. At last, a solution is proposed to mitigate those risks using risk management methodologies. Chapter four analyzes cyber security awareness programme definitions and concepts. It presents different approaches to establish a cyber security awareness programme. The concept and methodology for an awareness programme specific to children has also been presented. In chapter five, cyber security awareness programme for adolescents has been established using above selected approaches and methodologies.

1.9 Conclusion

Pakistan is one of the developing countries that is lacking the required level of security awareness at both levels of user ages: adults and children as the technology is advancing rapidly throughout these users. This research aims to target one user among these i.e. children. The security awareness programme proposed for the target group is based on the results of the survey conducted and security awareness topics from different international cyber security programmes already developed by different governments and organizations. The implementation of the cyber security awareness programme shall help bridge this gap for a better and secure potential cyber community. This chapter has covered the scope and objectives and how the research has been conducted.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

This chapter intends to investigate the present research on Pakistan's cyber space and its requirements to safeguard children from those risks. Already developed cyber security awareness programs specifically developed for children have been examined to assess the required acceptable level of awareness globally. Section 2.2 will present a relevance to the national need. Following this section 2.3 presents the compliance requirements of security awareness for all users discussing different standards and legislations. Finally, section 2.4 discusses the comparison between different cyber security awareness programs for children around the world.

2.2 Pakistan's Cyber Space

In the past, cyber security was only limited to information technology specialists. Through the current status, it has now become a collective obligation of grown-ups and kids. Pakistan is believed to hold the largest population of young children of around 18 years old in the world [6]. Though the target audience in the stated particular statistics are too young to be familiar with the cyber security concerns, yet they are the potential largest users of the cyber space.

In a paper by A. Bintziou et al., [9] they reported that there is a need to introduce IT-security awareness at this age because, when comparing the age of the secondary school students with first and second year university students; the later are already mapped with their way of thinking and practicing without caring to the issue of security. The article "Integrating Security into the Curriculum" argues "an educational system that cultivates an appropriate knowledge of computer security will increase the likelihood that the next generation of IT workers will have the background needed to design and develop systems that are engineered to be reliable and secure". [10]

As far as domestic cyber laws and regulations are concerned, Pakistan is lacking with essential requirements. National cyber security policy/strategy, E-Regulation and compliance, Criminal legislation, Roadmap for governance and Digital Pakistan policy

are all in the process of approval and yet to be finalized. Already developed Prevention of Electronic Crimes Act, 2016 [11] does not consider provisions or guidelines on cyber security awareness and training essential for the development of a cyber security workforce in the country. The draft Digital Pakistan policy 2017 [12] and draft National IT policy, 2016 [13] by Ministry of Information Technology enforces the need for indigenous development through a culture of cyber security for responsible user behavior and actions including capacity building and cyber security awareness campaigns.

2.2.1 Computer education in Pakistan

IT/Computer related material in books being taught in Pakistan does not focus on security related issues as much as required by the need assessment of usage, activities and interests of adolescents in Pakistan. The National curriculum for Computer Education for Grades VI-VIII [14] by Ministry of Education includes a brief unit of computer security threats encompassing definitions of Virus, Worm, Adware and Hacker and guidelines on managing an anitvirus. In view of the author, these definitions are not enough to provide adolescents the level of knowledge and skill they require to handle countless threats and issues while using the internet. No practical issues and risks have been covered in the education currirulum. This leaves the Pakistani children in a state of unconsciousness who are one of the largest potential users in the world.

2.3 Compliance requirements

Cyber security awareness raising is not a new concept and a lot of standards, frameworks and legislations have been developed by security departments and security researchers internationally on how to plan, develop and adopt an information security awareness program that encompasses the needs of a specific set of users.

a. **NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program** [15] **(NIST 2013)** This document aims to provide guidance for building an effective information technology security program. The guidance is presented in the form of a life-cycle approach. Consequently, the document puts forward four critical steps in the life cycle of an IT security awareness and training program. (1) Awareness and training program design, (2) awareness and training material development, (3) program implementation and (4) post-implementation. The document offers guidance on (a)

identifying training needs, (b) developing a training plan, (c) obtaining funding to the training program, (d) selecting training topics, (e) finding sources of training material, (f) implementing training material using a variety of methods, (g) evaluating the effectiveness of the program and (h) updating and improving the focus of the program.

b. **NIST Special Publication 800-16: A Role-Based Model for Federal Information Technology/Cyber Security Training** [16] **(NIST 1998)** The document presents a conceptual framework for providing information technology security training. The study argues that over time, employees acquire different roles relative to the use of information systems. Therefore, their need for security training changes as per those roles.

c. ISO/IEC 27001 & 27002 [17] are best practice guides to information security controls. It encompasses that all employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job functions.

d. **Federal Information Security Management Act (FISMA)** [18] FISMA is a United States Federal law enacted in 2002 and updated in 2014. The act recognized the importance of information security to the economic and national security interests of the United States. It considered security awareness training as essential as security itself and stated as below: -

§3544.(b).(4).(A),(B) – "*Security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities; and their responsibilities in complying with agency policies and procedures designed to reduce these risks."*

e. Released in 2009, the "*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure"* [19] by the Executive Office of the President, United States acknowledged the need for cybersecurity public awareness and an advanced cybersecurity workforce.

f. **EU Data Protection Regulation** [20] The European Union has directed all European member countries to develop and define laws regarding the protecting of personal privacy of the citizens of their respective country. While every country's implementation of this directive is different and unique, many of them require security awareness training to educate people on how to protect individual privacy.

2.4 Comparison of cyber security awareness programs

There is a variety of teaching resources on cyber security awareness topics for children offered on the Internet through various cyber security awareness programs. Many governmental organizations also developed appropriate resources for primary and secondary schools. A comparison of numerous cyber security awareness programs for children around the world has been made in Table 1 below to recognize the purpose of each resource and what topics and resources each program offer. The content of these resources could be utilized by parents and teachers for educational purpose and as a source material suitable for the awareness programme.

Table 1: Comparison of Cyber Security Awareness Programs of different Countries

Awareness programs	Content for Younger Kids	Content for Teens/Youth	Content for Parents/Adults
Cyber Safe (Malaysia) [21]	• Cyber Tips • Posters • Cyber Tools • Games & Quizzes	• Cyber Tips • Posters • Newsletter (Vol. 1-9) • Videos	• Cyber tips • Videos • Posters • Newsletters (Vol. 1-9)
Secure-Verify-Connect (Brunei) [22]	• **Learning Topics:** ➢ Online predators ➢ Internet addiction ➢ Cyber bullying ➢ Information security ➢ Identity theft	• **Learning Topics:** ➢ Cyber bullying ➢ Wireless security ➢ Viruses ➢ Safe Email Practice ➢ Social networking ➢ Social engineering ➢ Identity theft ➢ Using a shared computer ➢ Phishing ➢ Spyware ➢ Backup	• **Cyber Issues:** ➢ Keeping children safe ➢ Password management ➢ Using a shared computer ➢ Software security patches ➢ Cyber bullying ➢ Phishing ➢ Spyware

Awareness programs	Content for Younger Kids	Content for Teens/Youth	Content for Parents/Adults
	➢ Social engineering ➢ Social networking ➢ Computer security ➢ Internet security ➢ Email security ➢ Password ➢ Viruses ➢ kids play	➢ Password management ➢ Online grooming ➢ Internet addiction ➢ Computer security ➢ Internet security • Wallpapers • Digibytes (An Information Security Handbook)	➢ Wireless access points ➢ Antivirus software ➢ Firewall ➢ Backup ➢ Safe email practice ➢ Social networking ➢ Social engineering ➢ Identity theft ➢ Mobile phone security • Digi bytes (An Information Security Handbook) • Parent's guide to online safety • Posters
Go Safe Online (Singapore) [23]	-Nil-	• Articles • Securus (Publication) • Security Booklets • Posters	• Articles • Posters
Cyber Wellness (Singapore) [24]	• **Learning Topics:** ➢ Gaming Addiction ➢ Cyber Bullying ➢ Inappropriate Content	• Games	• Games • Video

Awareness programs	Content for Younger Kids	Content for Teens/Youth	Content for Parents/Adults
	➢ Netiquette ➢ Online Privacy ➢ Cyber Safety ➢ Cyber Security ➢ Copyright		
Savvycyberkids (US) [25]	• Lesson Plans • Activity sheets • Books	-Nil-	• Video Filter App
Digizen (UK) [26]	• Games • Things to do • Explore and learn • What you need to know	-Nil-	• What you need to know • Social Networking explained • Things to explore • Get creative • An In-depth look
RSA (Security division of EMC) [27]	-Nil-	• Videos • Podcasts	• Articles • Reports
Webwise (Ireland) [28]	-Nil-	-Nil-	• Advice • Explainers • How to • Publications • Teachers resources
Think u know (UK) [29]	• Cartoons • Games • Posters • Leaflets	• Videos • Need Advice • Got a question • Help	• Advices • Videos
Hacker Highschool (US)	-Nil-	• Books • Lessons 1-9	-Nil-

Awareness programs	Content for Younger Kids	Content for Teens/Youth	Content for Parents/Adults
[30]			
Get cyber Safe (Canada) [31]	-Nil-	• Cyberbullying Information for Teens • Online activities • Scams and frauds • Common threats • Videos • Web banners • Publications	• Protect your family • Protect your identity • Protect your money
CyberSmart.gov (Australia) [32]	• Get the facts • Get help online • Have Fun • Comic book capers • Draw a picture • Cybersmart gallery • How cybersmart are you? • Cybersmart access • Other fun websites • Videos • Gameon (Episodes 1-5) • NetBasics (Episode 1-10)	• How do I deal with: Issues? • I need to know about: Topics • Online help • Games and Videos • Posters • Animations	• Cyber issues • Resources • Educate yourself • Resources for young kids 4-7 years • Resources for kids 8-12 years • Resources for young Teens 13-18 years • Cyber security related websites • About the technology • Cyber safety guide
Netsmartz.org (US) [33]	• e-books	• Real life stories (Video) • Teens talk back (Video)	• Choose an issue • Videos

Awareness programs	Content for Younger Kids	Content for Teens/Youth	Content for Parents/Adults
	• Coloring pages • Trading cards • Cut-outs • T-shirts	• Report to cyberTipline	• Presentations • Teaching materials • Promotional items
NSTeens.org (US) [34]	-Nil-	• Videos • Games • Comics (2) • Quizzes	-Nil-
Staysafeonline.org (US) [35]	-Nil-	• C-save • Quizzes and games • Videos • Infographics • Tip sheets	• Raising Digital Citizens • Cyberbullying & Harassment • Parental Controls • Gaming Tips • Studies • Videos
ENISA [36]	-Nil-	• Video clips • Posters • Illustrations • Screen savers	• Posters for parents • Videos

2.4.1 Comparative Analysis

A large amount of security awareness material is available on different cyber security awareness programmes around the world for kids, parents and teachers. The content of these awareness campaigns is result of thorough research on the present risks to kids on the internet. The most common topics covered in these security programmes are: cyber bullying, internet addiction, online gaming, social networking, social engineering, mobile phone security, inappropriate content, netiquette, online privacy, viruses and safe email practice. A variety of media types have been used to circulate all the required knowledge to the target groups like tip sheets, posters, games, quizzes, newsletters, videos, handbooks, cartoons, mobile applications, leaflets, e-books. Resources for

parents and teachers include lesson plans, activity sheets, books, advices, explainers, articles, parental controls, parent's guides, teacher's guides.

There are numerous risks propagating online for adolescents due to the unidentified, abundant nature of the Internet and the level of communication it offers [5]. The results of the comparison of different cyber security awareness programmes around the world shows that the most common online risks to kids can be characterized into three broad categories – content, contact and conduct. Content risks include risks in which the kid is exposed to unauthenticated and mostly incorrect massive content. Contact risks include risks which may lead a kid to an undesired contact or disclosure of personal information during communication. Conduct risks include risks in which the kid may be the originator or performer of content or contact risks. The survey by the author investigates these categories in context of Pakistani school students and the results are discussed in the next chapter.

2.5 Conclusion

Rules and regulations for cybercrimes alone are not enough to build a good security posture among the internet users. A safe and secure behavior of these users is required to build a sensible workforce of internet users as described by different standards and regulations. This research has chosen adolescents as target audience owing to the fact that it's the youth who when trained on cyber security can build a prosperous country. Cybercrimes are on the rise in Pakistan and currently there are no efforts made to provide the young people appropriate awareness to keep them safe and secure online. This chapter has discussed various security awareness programmes worldwide that have made a difference in this field. Such awareness programmes and campaigns are so vital in developing countries as well in order to reduce the ratio of cybercrimes that happen every day in these countries due to lack of awareness among people.

Chapter 3

ONLINE RISKS FOR ADOLESCENTS

3.1 Introduction

This chapter aims to evaluate the present research on the risks and threats adolescents in Pakistan face over the Internet. Section 3.2 studies the nature of adolescents' usage behaviors and activities and their interests on the internet. Following this Section 3.3 will present a classification of such risks with an explanation and reasoning of each type. Using the information, the author presents the findings on the risks adolescents encounter in Pakistan based on the activities they participate in. Finally, in section 3.4, using a risk management approach the author identify a solution to empower adolescents handle these risks effectively.

3.2 Survey Methodology

The purpose of this survey was to obtain an overall understanding of how and why adolescents are accessing and using the Internet, to access parent's awareness of kid's online safety and to identify if these topics are being taught by teachers in the schools. Self-administered survey questionnaires were distributed to about 20 primary and secondary schools in Pakistan. The subjected schools were selected from all kinds of schools in Pakistan including: Public, Private local, Private International and Military. There were three different questionnaires each designed for a different target audience; adolescents in schools aged between 12 and 18, parents of those adolescents and their teachers.

3.2.1 Tools

While there is an extensive variety of sample questionnaires already prepared on this topic for example by SANS Technology Institute [37], a new questionnaire was prepared by the author of this study. This questionnaire was planned with the research objectives of the author in mind. The author also considered the fact that adolescents were self-administering the questionnaires and the complications in gathering required information from this audience. The survey tools were established following a literature review to develop their content rationality.

1) Questionnaire for adolescents aged 12 – 18 (Appendix A)

This questionnaire comprised of six sections of questions and was aimed at gathering information about adolescent's online habits; regularity of access, location of access, online activities and their awareness of certain risks categorized in literature review and related security and safety controls.

2) Questionnaire for parents (Appendix B)

This questionnaire which consisted of ten questions was intended to obtain an overall understanding of parent's attitudes and behaviors about their kid's internet access and some technological security features.

3) Questionnaire for teachers (Appendix C)

This questionnaire was developed to gain information about school teacher's usage of the internet with adolescents and their knowledge of children e-safety initiatives already developed and in use.

3.2.2 Pilot study

A pilot study included ten adolescents aged between 12 and 18, five parents and five teachers recognized the validity of the questionnaires and acknowledged the necessity for minor changes. The re-established questionnaire was piloted on an additional five respondents in each category. No issues with understanding or completion were observed.

3.2.3 Sampling frame

Contact was made with previous university and work colleagues to ascertain their interest and availability to participate in the survey. The study population was divided into three categories; primary and secondary school adolescents aged between 12 and 18, parents of the sampled kids and their school teachers.

3.2.4 Survey response

Of the total of 500 questionnaires circulated to adolescents aged between 12 and 18, 405 surveys were returned after completion (81% response rate). Of the total of 60 questionnaires circulated to parents of this same population, 33 were completed and returned (55% response rate). Of the total 60 questionnaires circulated to school teachers, 53 completed surveys were returned (88.3% response rate).

3.2.5 Data analysis

Data analysis was made using SPSS [8]. Data was entered into data spreadsheets using customized variables, checked for errors by comparison with raw data, and updated as required. Data was then analyzed using statistical formulas. A few charts were made with the help of Microsoft Excel. Responses to the open survey questions were captured physically and subsequently submitted into frequency tables.

3.3 Adolescents' interests online and nature of internet usage

This section will identify how adolescents in Pakistan are using the internet, the activities they perform online and the nature of their internet access which will provide a fair glimpse of cyber security risks they may face. The purpose of internet usage and actions will determine the type of risk they are vulnerable to and the nature of their access will have a bearing on their exposure to the online risk.

3.3.1 Research to date

A lot of research has been carried out on the relationship between children and the Internet in the west [3] [4] [5]. The EU Kids Online Network published a report [3], categorizing the study carried out on young kids' access to and usage of the Information and Communication Technologies across Europe. The report described that the most investigated issues are internet usage ratio proceeded by access, interests and activities. Other parts of research are constructed on kids' online expertise, online social networking, online gaming, the after effects on children for surfing online, and worries and obstructions of kids. By far, no research has been carried out in Pakistan for this target group in this regard. The author has tried to raise all these research questions with specific scope to Pakistani children.

3.3.2 Kids online activities

The European Commission's Safer Internet for Children Qualitative Study [38] which was carried out in 29 countries in Europe discovered that the access to the Internet by children is made for two key purposes; for playing online games and looking for information on topics they are attracted towards, also includes internet surfing for entertainment. It also discovered that looking for information for homework, communication with friends and family, downloading music and sending and receiving emails and files are also regular actions performed by the children.

The survey by the author considering Pakistani school children, reported that the most widespread activities that kids participate in over the internet are looking up information for schoolwork (54.3%), social networking (Facebook, Twitter etc.) (49.4%), downloading pictures/audios/videos (37%), online gaming (30%), sharing pictures and information (25.7%), surfing/browsing web pages (25%), and communications (email, instant messaging etc.) (20%). It was also noted that social networking has become a daily activity for most children (58%), particularly adolescents.

Table 2: Do you use the internet for looking up information for schoolwork?

Answer	Occurrence	Percent	Collective Percent
No	185	45.7	45.7
yes	220	54.3	100.0
Total	405	100.0	

Table 3: Do you use the internet for social networking (Facebook, Twitter etc.)?

Answer	Occurrence	Percent	Collective Percent
No	205	50.6	50.6
yes	200	49.4	100.0
Total	405	100.0	

Table 4: Do you use the internet for downloading pictures/audios/videos?

Answer	Occurrence	Percent	Collective Percent
No	255	63.0	63.0
yes	150	37.0	100.0
Total	405	100.0	

Table 5: Do you use the internet for online gaming?

Answer	Occurrence	Percent	Collective Percent
No	284	70.1	70.1
Yes	121	29.9	100.0
Total	405	100.0	

Table 6: Do you use the internet for sharing pictures and information?

Answer	Occurrence	Percent	Collective Percent
No	301	74.3	74.3
yes	104	25.7	100.0
Total	405	100.0	

Table 7: Do you use the internet for communication (Email, instant messaging)?

Answer	Occurrence	Percent	Collective Percent
No	325	80.2	80.2
Yes	80	19.8	100.0
Total	405	100.0	

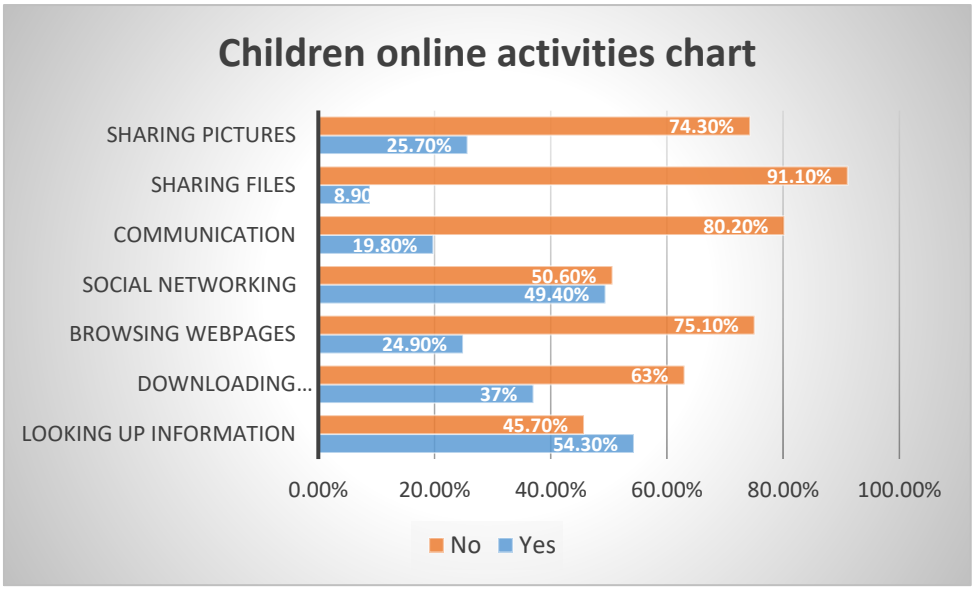

Figure 1: Online activities of children in Pakistan

3.3.3 The nature of internet usage

In order to examine the subject of online risks, it is vital to evaluate the nature of kids' internet usage as this will impact a kid's vulnerability to these risks.

a. Access locations - Increase from home

In the study carried out by this author, it was found that the number of children accessing the Internet from their own homes has been increased which is an emerging change. It was informed that the most common location of access to the internet was at home (69.4% n=405) followed by location at school (30.6%). 9.9% of adolescents responded that they use the internet at friend's home while 7.9% of them uses it at

relative's home. A mere total of 3% uses the internet at internet cafes. Research has shown that kids who found access to the internet at home practice it on a more regular basis [3]. This growth in access at home is due to the reason that since we live in a risk occupied culture, children are more forbidden to play outdoors and are being limited indoors. For the purpose of entertainment and engagement for them, parents are trying to provide them a rich media environment at home.

Table 8: Do you access the internet at home?

Answer	Occurrence	Percent	Collective Percent
no	124	30.6	30.6
yes	281	69.4	100.0
Total	405	100.0	

Table 9: Do you access the internet at School?

Answer	Occurrence	Percent	Collective Percent
no	281	69.4	69.4
yes	124	30.6	100.0
Total	405	100.0	

Table 10: Do you access the internet at internet cafe?

Answer	Occurrence	Percent	Collective Percent
no	393	97.0	97.0
yes	12	3.0	100.0
Total	405	100.0	

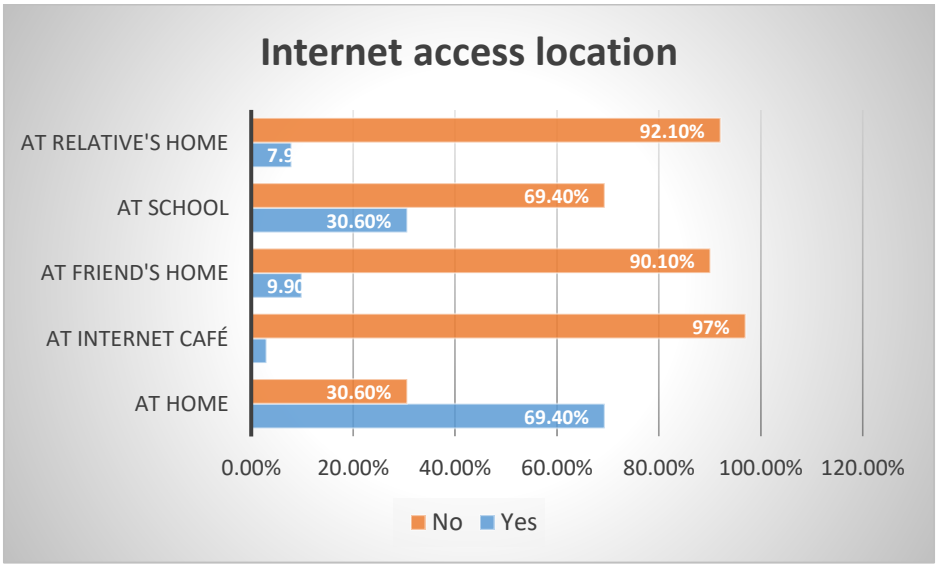

Figure 2: Location of internet access

b. Access at younger age

The study by the author also provides evidence that adolescents are accessing the internet from an earlier age and the conception has been anticipated that this inclination will continue with the likelihood of kids beginning to access the Internet as soon as they begin walking.

Table 11: Age-wise internet usage Crosstabulation

		Usage				Total
		Everyday	Weekends	Once a week	Rarely	
Age	12	4	8	8	0	20
	13	13	11	0	25	49
	14	23	4	12	44	83
	15	41	10	9	30	90
	16	21	5	8	20	54
	17	29	7	12	10	58
	18	31	6	3	11	51
Total		162	51	52	140	405

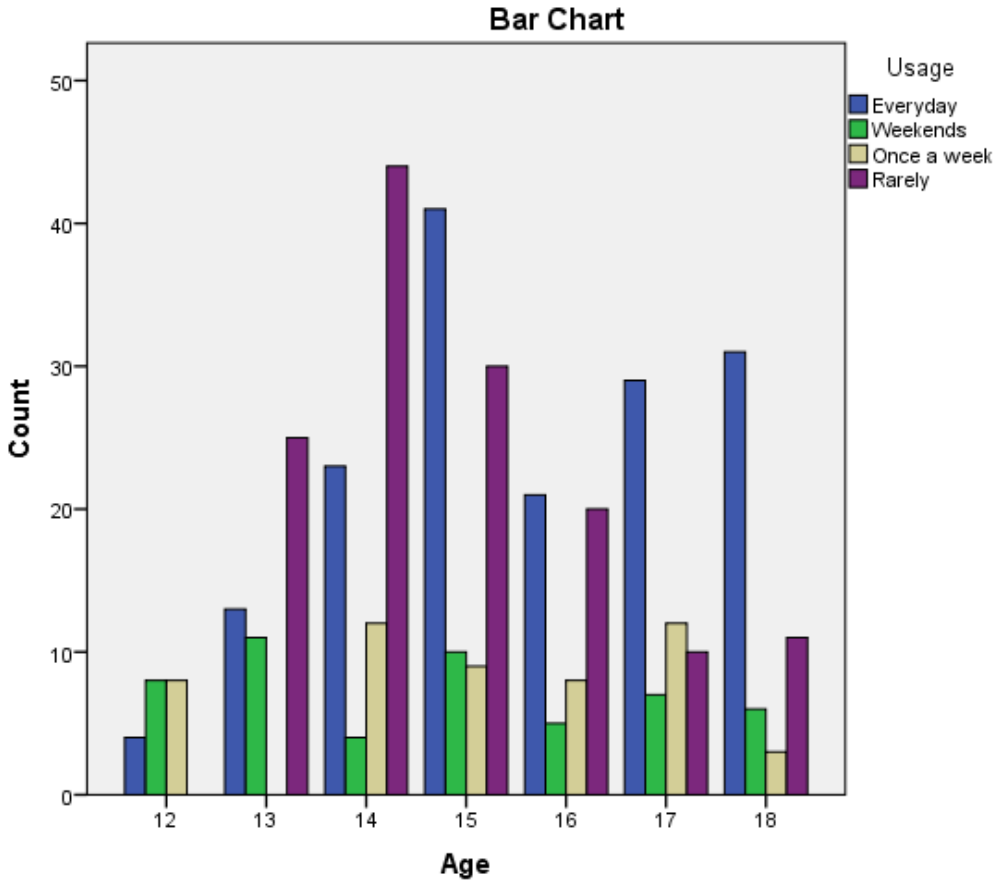

Figure 3: Age-wise internet usage graph

c. Learning process – Self-learning

Children in the survey revealed that they have learnt to use the internet primarily by self-learning with some contribution to explain them the basics from teachers or elder siblings at the beginning. In general, most adolescents claimed that they have learnt to access the internet through themselves. Almost half of the sample respondents declaring that they have educated themselves at their own how to access and use the internet for various purposes (47.7%). School teacher was the second most basis for learning to use the Internet (20.7%) followed by siblings (14.8%). Only 7.9% (n=405) declared that they have learned to use the Internet from their parent.

Table 12: Who has shown you how to use the Internet?

Answer	Occurrence	Percent	Collective Percent
Parents	32	7.9	7.9
School Teacher	84	20.7	28.6
Self-learning	193	47.7	76.3
Brother/Sister	60	14.8	91.1
Friends	36	8.9	100.0
Total	405	100.0	

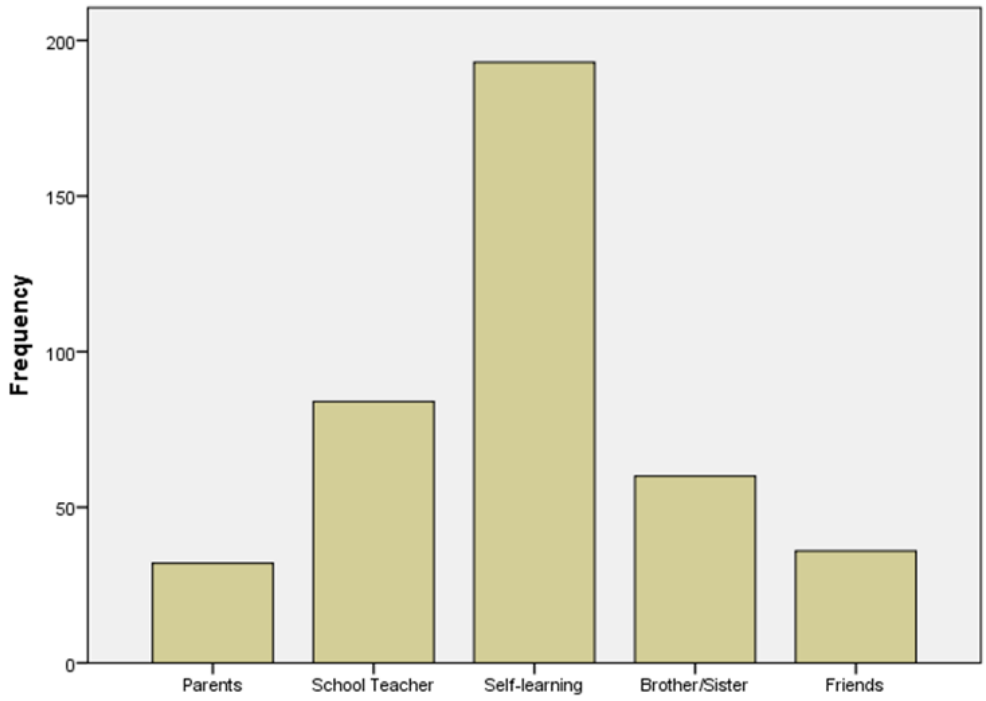

Figure 4: Learning process contribution check graph

3.3.4 Consequences

Increase in the nature of access of adolescents using the Internet from home may increase the ratio of kids' use of the Internet which in turn may result in growth of their exposure to online risks. The more often a kid uses the Internet the more possible for him/her that he/she will face risks. Kid's age is also a significant factor in determining the impact of the risk on the child. As concluded above, adolescents access to the Internet is more frequent at a younger age which establishes the fact that they will be more exposed to certain types of risk as they will not be possessing as much skills and capability to handle the variety of internet risks.

The source through which children learn to access and use the Internet will have an effect on the possibility of evolving good Internet practices. As the higher ratio of adolescents are learning to use the Internet at their own, it is very doubtful that they will progress in developing good and safe Internet behaviors than if they were learning from an expert user of the internet.

3.4 Risks for adolescents over the internet

There are many risks propagating online for adolescents due to the unidentified, abundant nature of the Internet and the level of communication it offers [5]. The survey by the author categorizes online risks to kids into three categories – content, contact and conduct. Content risks include risks in which the kid is exposed to unauthenticated and mostly incorrect massive content. Contact risks include risks which may lead a kid to an undesired contact or disclosure of personal information during communication. Conduct risks include risks in which the kid may be the originator or performer of content or contact risks. The survey by the author investigates these categories in context of Pakistani school students and the results are discussed below.

3.4.1 Contact risks

a. Undesirable contact

With the rise in usage of social media networking, which provide adolescents to connect and collaborate with family, friends, public or private social groups, and other people around the world by means of social media tools (i.e. Facebook, Twitter, MySpace, Instagram and YouTube etc.) and instant messaging services (i.e. WhatsApp, Skype, Viber, Facetime etc.), adolescents are the largest potential target group of getting

undesirable and inappropriate contact from strangers and even from friends playing as cyber bullies [39]. Below is an overview of these risks.

i. Strangers / Criminals: These are people who start online relationships with adolescents for the purpose of taking benefit of them. Once they succeed in gaining trust of the adolescent, they may request for images, personal information and eventually to meet in person. A couple of incidents have been already happened in Pakistan where adolescents have been kidnapped for ransom by the criminals after establishing contact and confidence building on the internet via social networking websites.

ii. Friends: These are persons already known to the children, and are mostly other children at the same school. Friends can threat a kid by bullying online. As of today, bullying is not just physical clash anymore. Online bullying can be as offensive as it could be due to the anonymity factor and the attacks can be both violent and public.

iii. Themselves: In the current digital era of social networking, the worst enemy of adolescents can be themselves. Anything they publish is not only reachable to the whole world, but also may be hard or sometimes impossible to eradicate. Adolescents may not understand how these postings can affect their forthcoming lives.

The results of the survey by the author show that a good ratio of adolescents responded that they should only add people to their friend lists who they are sure they know on social networking sites. But the conduct of the adolescents does not support the response. 43% of adolescents responded that their online profile is not private or no restrictions have been applied to safeguard their sensitive or personal information.

Table 13: What kind of people you are interested to add to your friend list on Social Networking Services (SNS) like Facebook etc.?

Answer	Occurrence	Percent	Collective Percent
Someone who looks familiar	96	23.7	23.7
People I am sure I know	263	64.9	88.6
Anyone, I don’t care	46	11.4	100.0
Total	405	100.0	

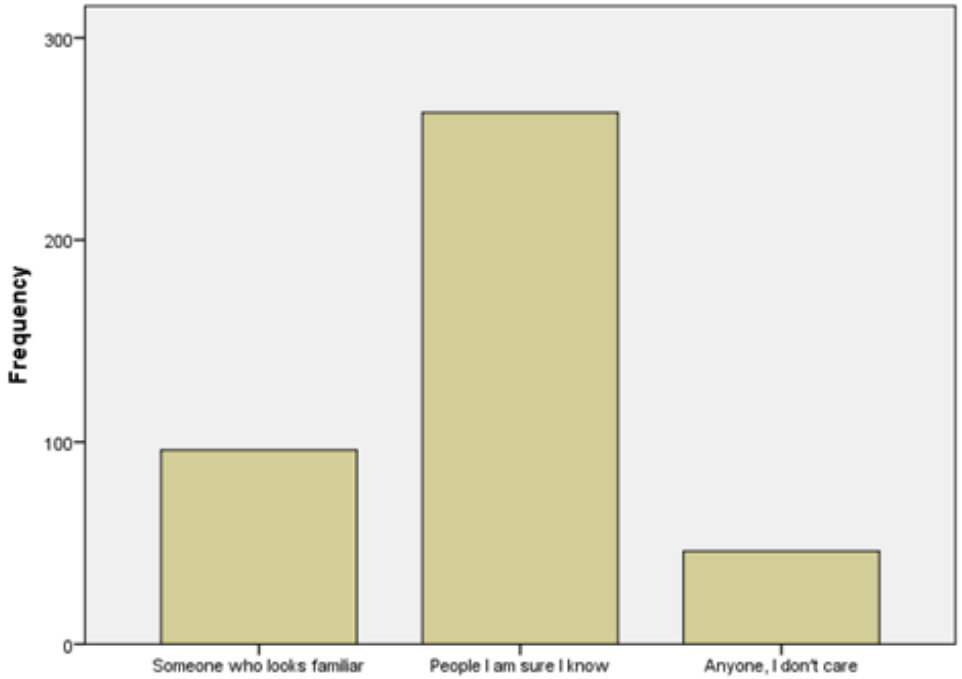

Figure 5: Contacts to add on Social networks check graph

Table 14: Is your Profile Private?

Answer	Occurrence	Percent	Collective Percent
Yes	164	40.5	40.5
No	172	42.5	83.0
Don't know	69	17.0	100.0
Total	405	100.0	

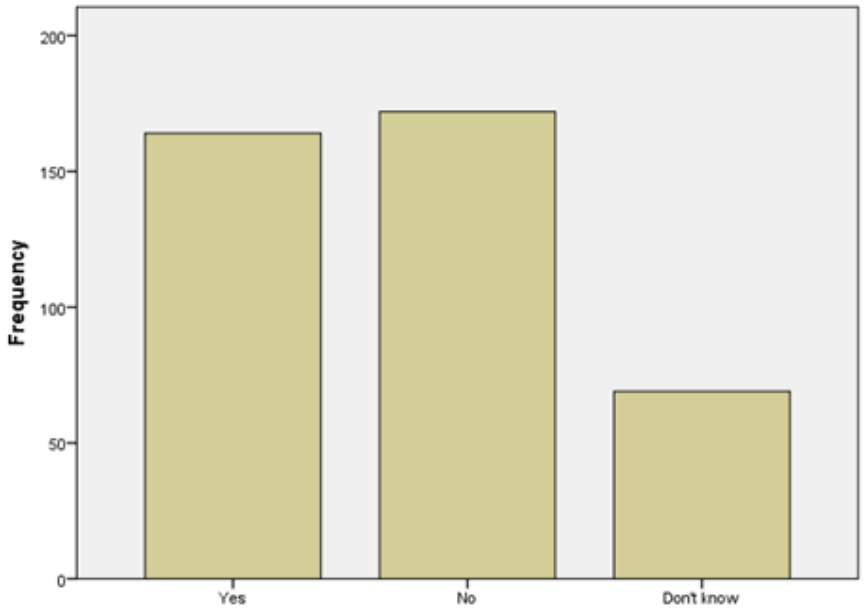

Figure 6: Private Profile check graph

The survey also revealed that 30% of the adolescent respondents have received threatening calls or messages from strangers who can be criminals. When interviewed about the nature of threatening calls or messages, the adolescents responded that most of the times they faced cyber bullying and sometimes inquiries about their personal information.

Table 15: Have you ever received threatening calls or messages from someone?

Answer	Occurrence	Percent	Collective Percent
Yes	121	29.9	29.9
No	256	63.2	93.1
Don't know	28	6.9	100.0
Total	405	100.0	

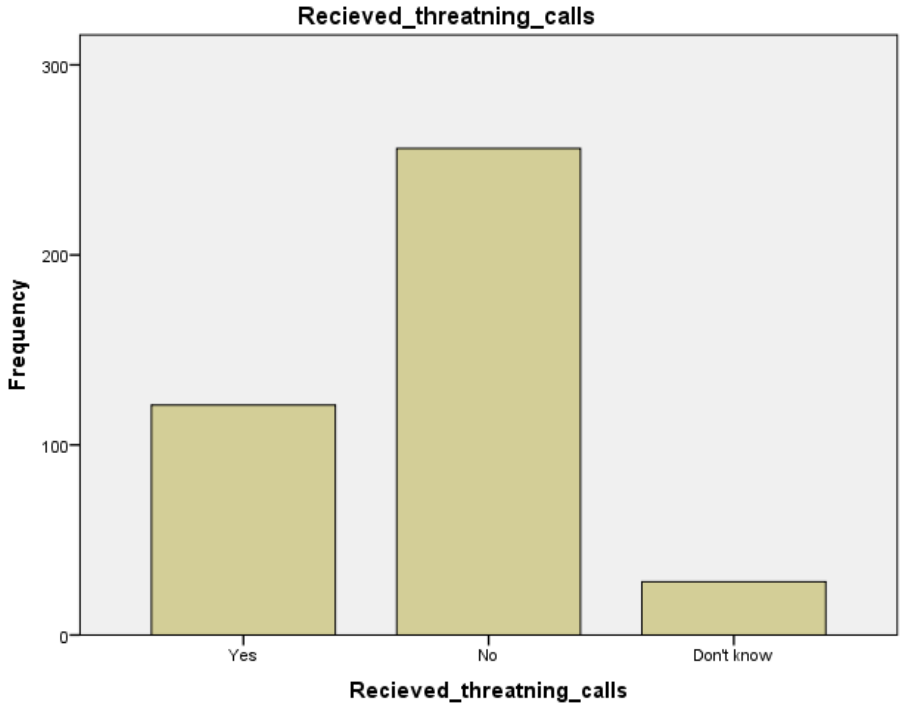

Figure 7: Threatening calls and messages check graph

b. Disclosure of Personal information

Adolescents are posting their personal information on the Internet ever more than ever before via social networking sites and public or group blogs. Children do not possess enough awareness to understand that new friends made on the internet may not be in real who they claim they are and that once a person is added as a friend to an online profile account, it is evident that he can gain access to children's personal information without trouble. Adolescents may be unaware of the dangers linked with the disclosure

of sensitive or personal information. This can lead to a variety of risks including but not limited to phishing attacks, social engineering or being receivers of unsuitable marketing therefore increasing the likelihood to undesired contact.

In the survey, the author asked adolescents who do they feel is effective at helping them maintain the online security, privacy and safety of their personal information online. Majority of them (around 45%) believed that to be themselves but when asked about what kind of information they share on the internet without their parent's permission, they lack desired awareness level. 90% of them believed that there is no harm in sharing phone number or school name and address over the internet with anyone. Also, 47% of the adolescents believe the same for sharing family details and information which is a significant sign of low awareness level among adolescents in Pakistan.

Table 16: Who do you feel is effective at helping you maintain the online security, privacy and safety of your personal information online?

Answer	Occurrence	Percent	Collective Percent
Self	184	45.4	45.4
Online companies	44	10.9	56.3
Parents	54	13.3	69.6
Governments	19	4.7	74.3
Schools	92	22.7	97.0
Teachers	12	3.0	100.0
Total	405	100.0	

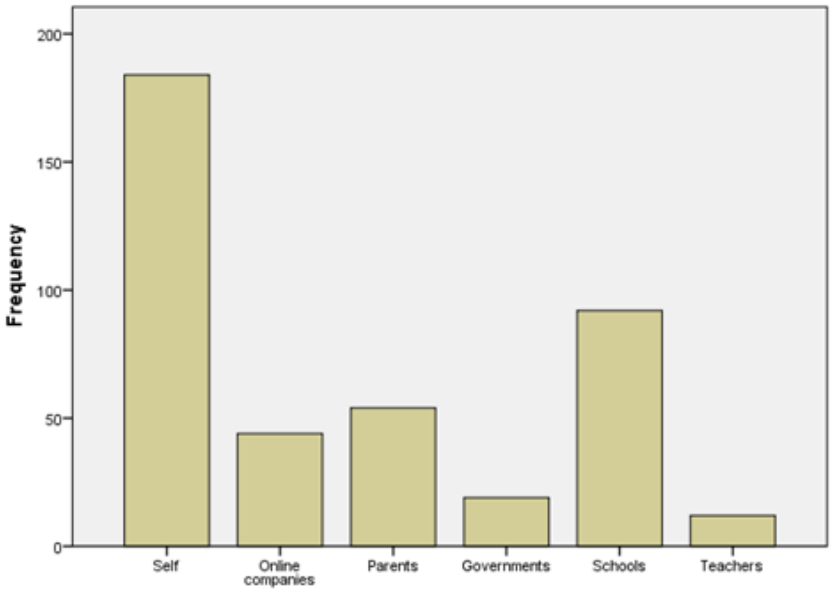

Figure 8: Personal information security responsibility check graph

Table 17: Do you require your parent's permission before sharing information about your phone number or school name & address over the internet?

Answer	Occurrence	Percent	Collective Percent
no	364	89.9	89.9
yes	41	10.1	100.0
Total	405	100.0	

Table 18: Do you require your parent's permission before sharing family details over the internet?

Answer	Occurrence	Percent	Collective Percent
no	176	43.5	43.5
yes	229	56.5	100.0
Total	405	100.0	

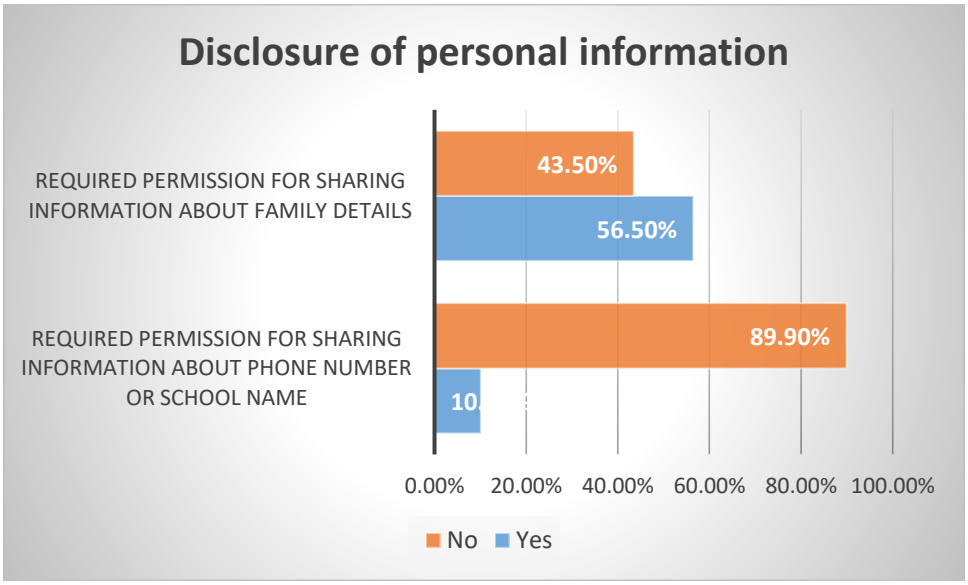

Figure 9: Parents' permission for sharing family information check graph

3.4.2 Content risks

A large amount of online content is not appropriate for adolescents and can be upsetting or damaging. This is correct for content accessed and observed via blogs, web pages, social media networks and online gaming. The risks involved are stated below with reasoning.

a. Ambiguous content

This type of risk arises due to the fact that now any user can upload their own content to the Internet. This material can be uploaded to social networking sites, blogs,

unauthenticated information portals, and in public discussion forums. This content is not examined by specialists or authorities to verify its correctness or otherwise. There exists no definite place where “editorial control” on this user-created material can be assured [5]. It is very unlikely to control the flow of content that is uploaded on the Internet. Due to which, it is possible for children to obtain wrong or biased information when they surf the internet. The author asked the adolescents about the benefits of internet. 61.2% of children responded that learning is the greatest benefit the internet has brought to their lives. The ambiguity of the information and knowledge on the internet may affects the learning process and children may be on the wrong track of learning without any knowledge.

Table 19: Does Learning the greatest benefit the internet has brought to your life?

Answer	Occurrence	Percent	Collective Percent
no	157	38.8	38.8
yes	248	61.2	100.0
Total	405	100.0	

Table 20: Does Socializing the greatest benefit the internet has brought to your life?

Answer	Occurrence	Percent	Collective Percent
no	285	70.4	70.4
yes	120	29.6	100.0
Total	405	100.0	

Table 21: Does Exploring the greatest benefit the internet has brought to your life?

Answer	Occurrence	Percent	Collective Percent
no	290	71.6	71.6
yes	115	28.4	100.0
Total	405	100.0	

Table 22: Does Entertainment the greatest benefit the internet has brought to your life?

Answer	Occurrence	Percent	Collective Percent
no	183	45.2	45.2
yes	222	54.8	100.0

Answer	Occurrence	Percent	Collective Percent
Total	405	100.0	

Table 23: Does Contacting the greatest benefit the internet has brought to your life?

Answer		Occurrence	Percent	Collective Percent
Valid	no	273	67.4	67.4
	yes	132	32.6	100.0
	Total	405	100.0	

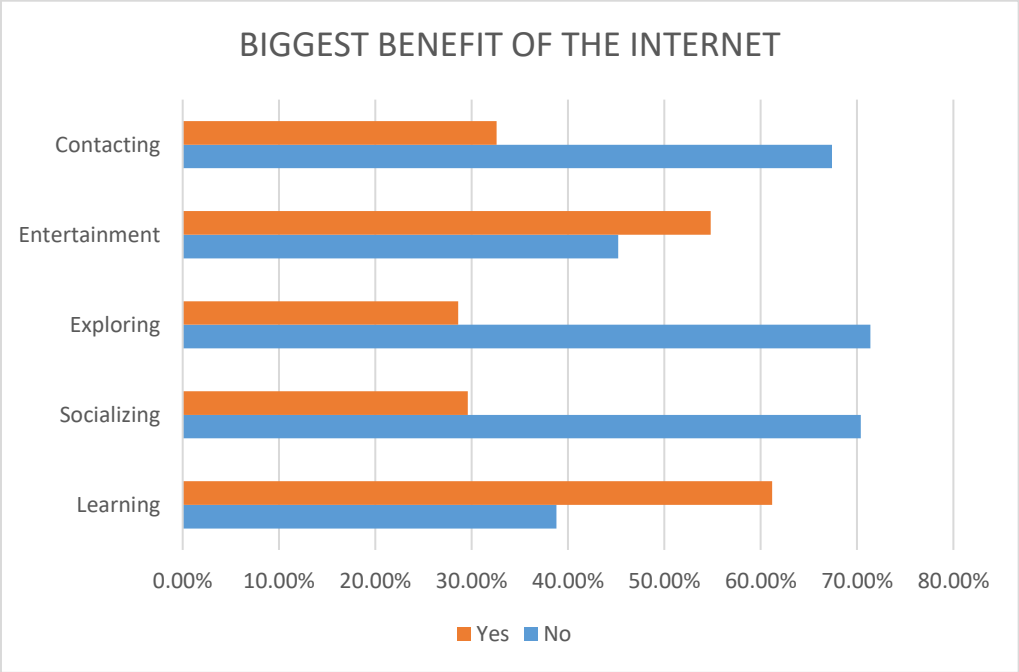

Figure 10: Learning benefit check graph

46.7% of the adolescents in schools believe that the information on the internet is always correct. Around 17% do not know whether it is correct or not. Young users with no prior knowledge are vulnerable to this risk as they do not find any assistance to reduce this risk and may believe the information to be true in all instances.

Table 24: Does the information on the internet always correct?

Answer	Occurrence	Percent	Collective Percent
Yes	189	46.7	46.7
No	149	36.8	83.5
Don't know	67	16.5	100.0
Total	405	100.0	

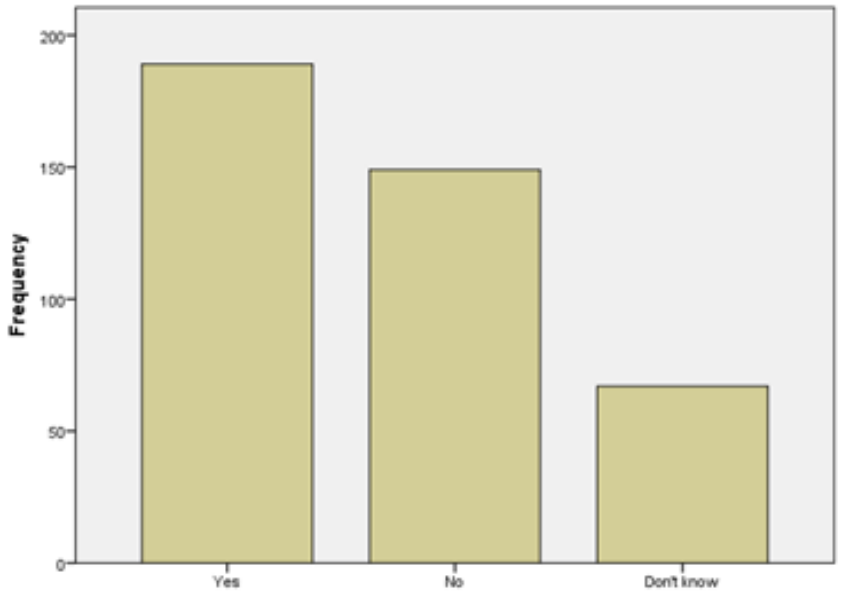

Figure 11: Information correctness check graph

b. Lack of age-wise content

Internet provides a plenty of information for its extensive variety of users. This information is simply available to all users and can be send quickly and easily to any user around the world. Nevertheless, most of this information is not suitable for users of all ages and adolescents are exposed to it by showing up to this kind of information deliberately or mistakenly. A study [38] in UK showed that less than one-third of frequently viewed websites by children are actually designed for children. This means that most of the content available is not suitable for children, therefore increases the probability of content risk. There is an abundance of information available on the Internet that should be classified and marked as unsuitable for kids.

Age-wise unsuitable content consists of illegitimate content such as nudity or racist material, through to damaging material which includes hateful material to violent content. The survey reveals that most adolescents use internet at their home which reduces the above-mentioned risk of exposure to adolescents.

Table 25: Do you access internet at home?

Answer	Occurrence	Percent	Collective Percent
no	124	30.6	30.6
yes	281	69.4	100.0
Total	405	100.0	

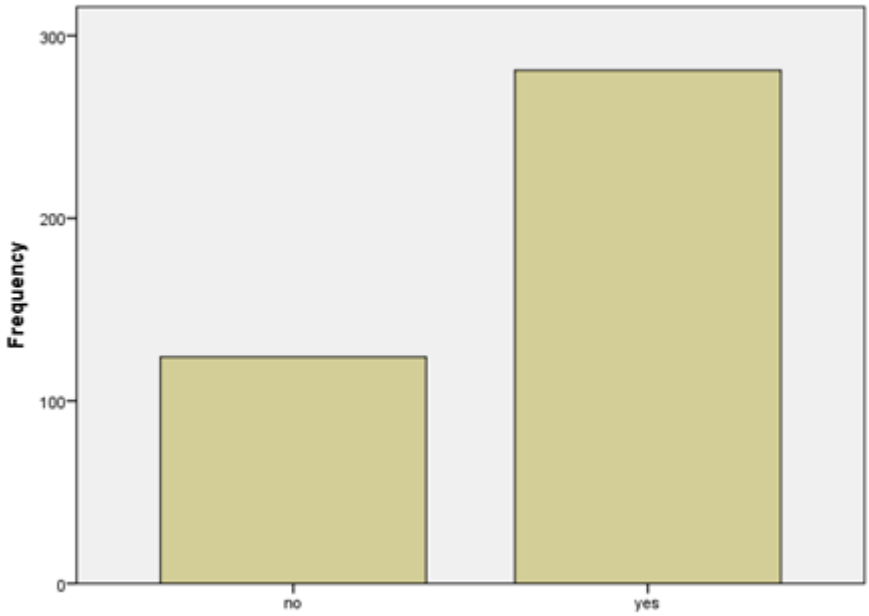

Figure 12: Internet access at home check graph

Yet about 48% of the respondents claim that they have learned to use the internet by themselves. When interviewed, they narrate that the internet is an open play ground where they can access any kind of information without considering appropriateness or relevance. This can lead them to exposure of content that is morally, ethically or legally forbidden for them.

Table 26: Who has taught you how to use the internet?

Answer	Occurrence	Percent	Collective Percent
Parents	32	7.9	7.9
School Teacher	84	20.7	28.6
Self-learning	193	47.7	76.3
Brother/Sister	60	14.8	91.1
Friends	36	8.9	100.0
Total	405	100.0	

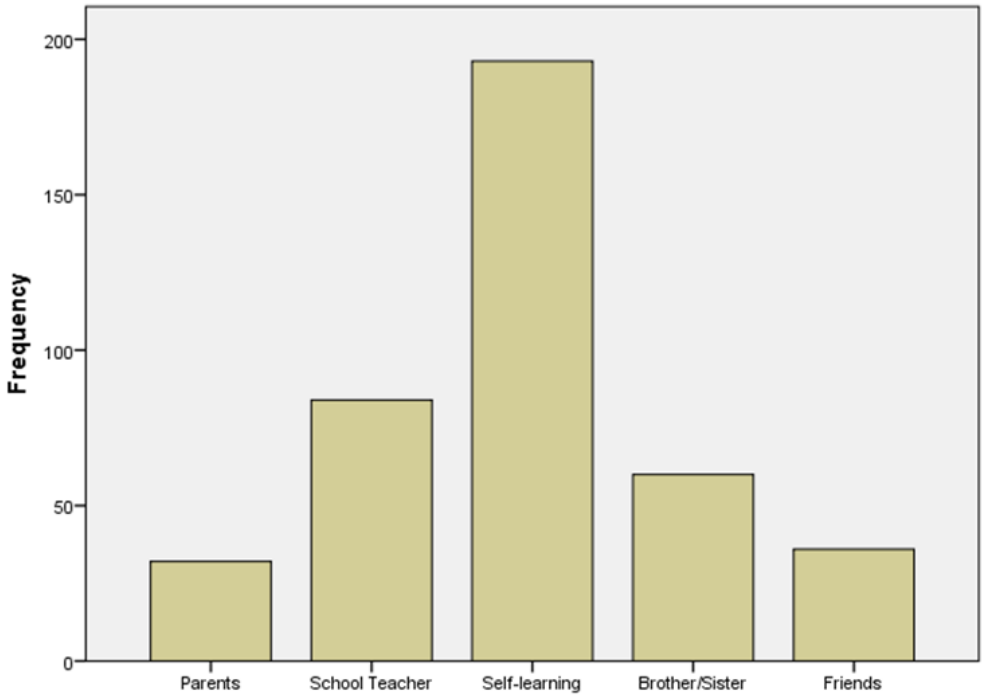

Figure 13: Learning process contribution check graph

c. Commercialism

Children's privacy and entertainment on the internet can sometimes face hindrance and interference by promotional and advertising schemes, which means involuntarily costing money online, such as through applications. The study in UK [38] also disclosed that 95% of the most visited websites by children do contain some kind of commercial material. This type of material includes promotional content for selling products and services, advertising, junk and funding content. Children are exposed to this type of risk as they do not possess the literacy skills about media to deal well with this material.

Table 27: How much time do you spend on the Internet daily?

Answer	Occurrence	Percent	Collective Percent
Half an hour	228	56.3	56.3
One hour	85	21.0	77.3
Two hours	52	12.8	90.1
Four hours	24	5.9	96.0
More than five hours	16	4.0	100.0
Total	405	100.0	

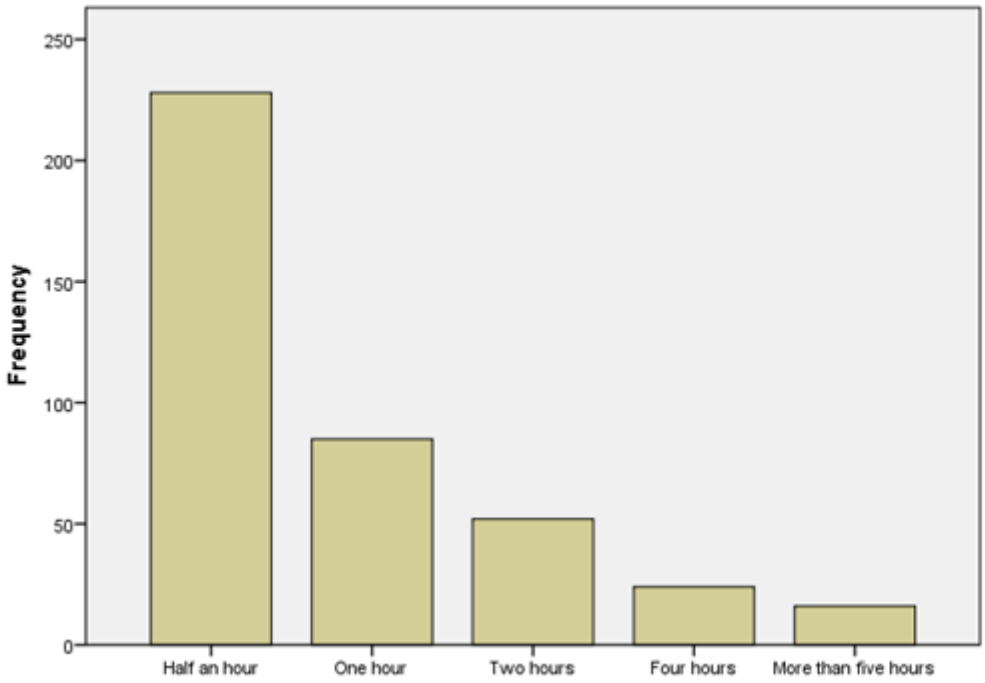

Figure 14: Internet usage duration check graph

The survey revealed that around 57% of the respondents spend more than half an hour daily on the internet. During this time, they are well exposed to the commercial content which may not target them as potential viewers in most cases. Also, same ratio of adolescents spends same amount of time on Facebook which is also a hub of advertising schemes and marketing. 1.32 billion daily active users on average for June 2017 [40] are exposed to commercial content on Facebook among which proportion of young people can be imagined. Spamming hidden links in advertisements may lead to undesired websites to obtain personal information.

Table 28: How much time do you spend on Facebook daily?

Answer	Occurrence	Percent	Collective Percent
None	26	6.4	6.4
Half an hour	235	58.0	64.4
One hour	76	18.8	83.2
Two hours	48	11.9	95.1
Four hours	8	2.0	97.0
More than Five hours	12	3.0	100.0
Total	405	100.0	

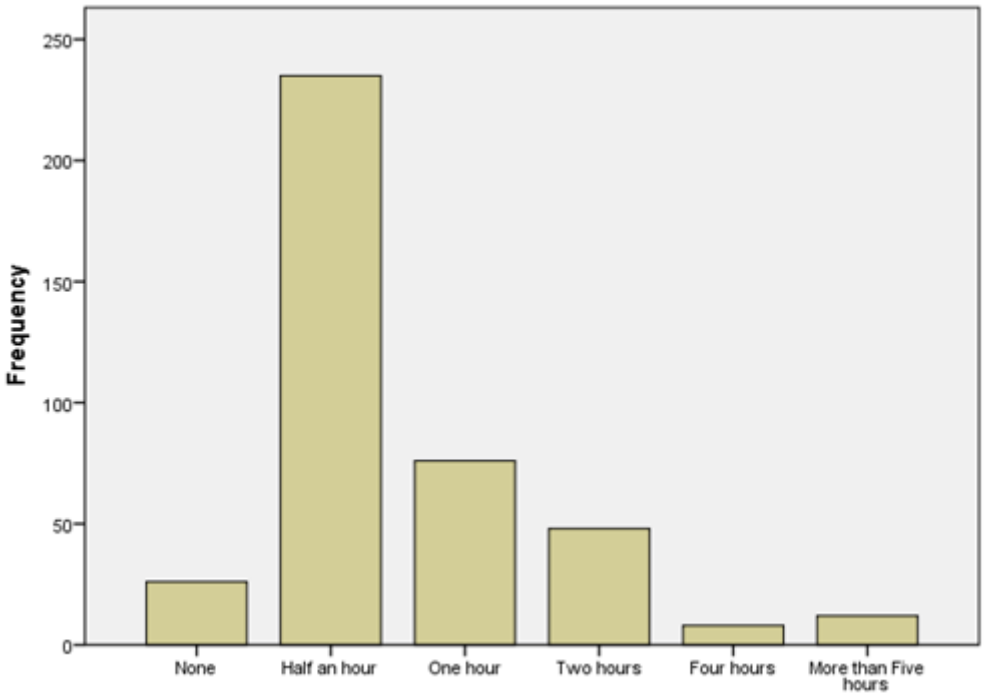

Figure 15: Facebook usage duration check graph

3.4.3 Conduct risks

A majority of children are not aware of the fact that their online activity can have an impact on themselves as well as on other people, and the digital footprint that they mark online. It is very simple to feel anonymity online and it is important that adolescents know that each of their activity on the internet can be track back to them, if needed. In a statistic by Microsoft in 2016 [41], 70% of United States job recruiters have rejected applicants based on their online reputations. Also, casual, unethical or unsafe conduct can lead them to an exposure of a severe threat.

The survey by the author establishes the fact that adolescents are well careless about their conduct on the internet. 35.6% of the children responded that they have never changed their password since it was created the very first time. 14.1% believed that it's not important to change their password at all, so there is no need for that. 16.8% responded that they change it once in a year.

Table 29: How many times did you change your password?

Answer	Occurrence	Percent	Collective Percent
Never Changed	144	35.6	35.6
Everyday	4	1.0	36.5

Answer	Occurrence	Percent	Collective Percent
Once a week	20	4.9	41.5
Once a month	112	27.7	69.1
Once a year	68	16.8	85.9
Never believed its important	57	14.1	100.0
Total	405	100.0	

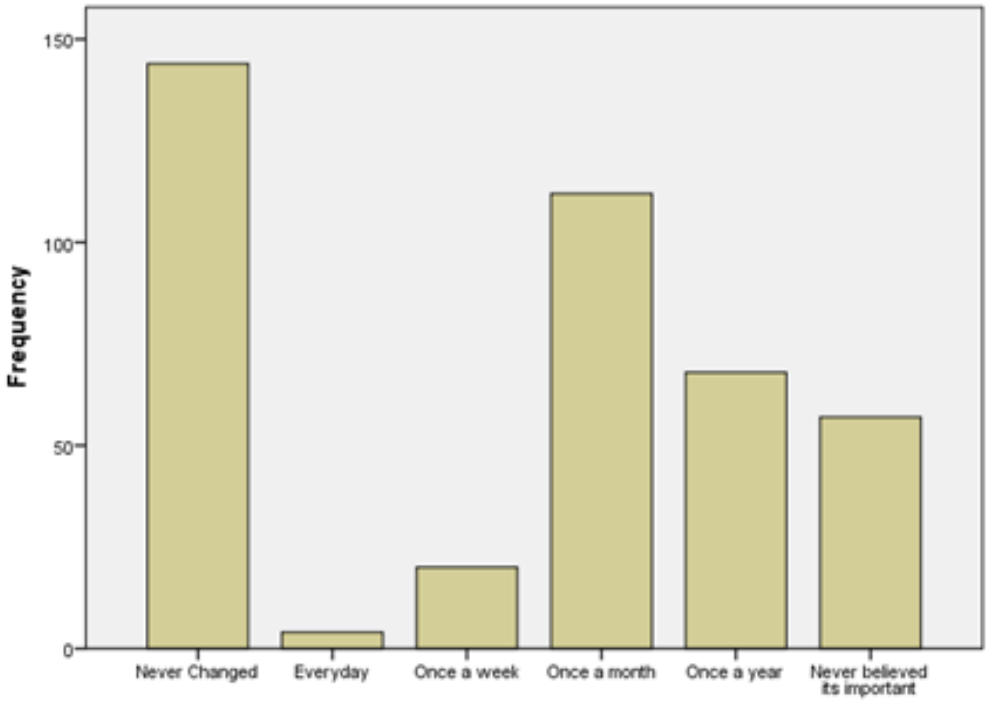

Figure 16: Changing passwords frequency graph

When asked about their conduct regarding location sharing on mobile devices, 66.4% of adolescents replied that they do not regularly turn off their location and wi-fi services after using them. This conduct can make their mobile devices vulnerable and their physical location exposed to the adversaries.

Table 30: Do you regularly turn off your Wi-Fi, Bluetooth and location services after usage?

Answer	Occurrence	Percent	Collective Percent
Yes	88	21.7	21.7
No	269	66.4	88.1
Don't know	48	11.9	100.0
Total	405	100.0	

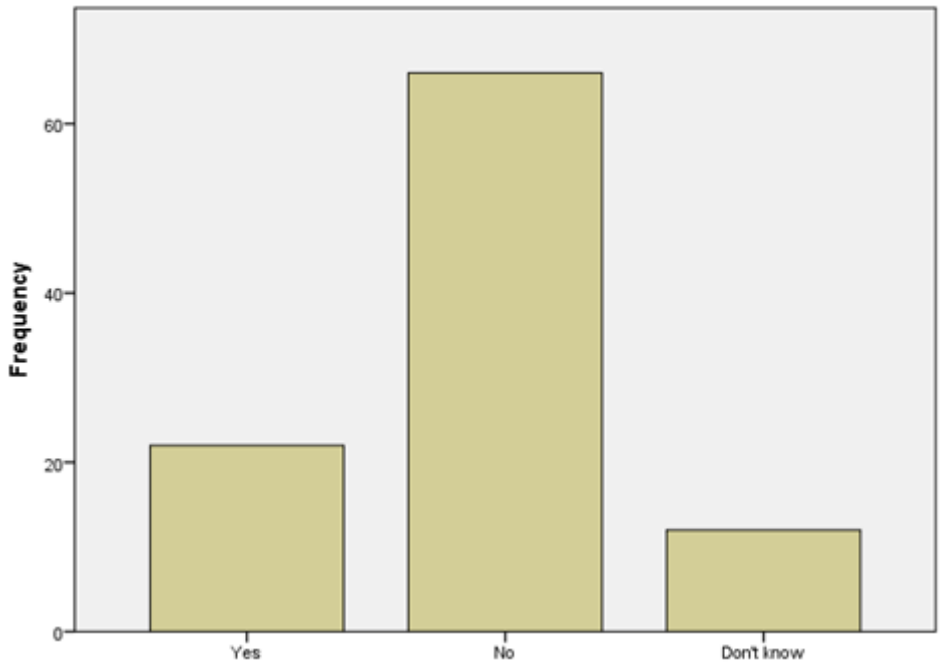

Figure 17: GPS services enabled check graph

Another risk regarding to children's conduct is illegal downloading and use of proxies to bypass any kinds of restriction filters. Children are unaware of the legal and moral restrictions of software usage and access to restricted/controlled content. Newly constituted Prevention for Electronic Crimes Act, 2016 in Pakistan [11] enforces clear obligations in this regard. Still 25% of the children responded that they use pirated software and 17% replied that they use proxy software to circumvent the restrictions/filters to access controlled websites.

Table 31: Do you use pirated and cracked software on your devices?

Answer	Occurrence	Percent	Collective Percent
Yes	100	24.7	24.7
No	197	48.6	73.3
Don't know	108	26.7	100.0
Total	405	100.0	

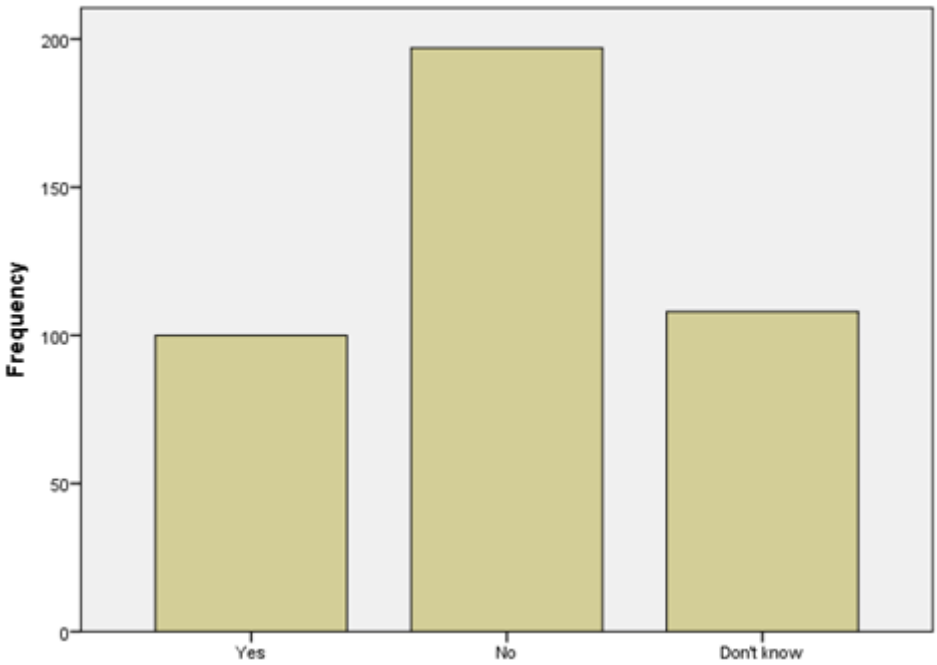

Figure 18: Pirated/Cracked software usage check graph

Table 32: Do you use proxies for accessing restricted websites like YouTube*?

Answer	Occurrence	Percent	Collective Percent
Yes	68	16.8	16.8
No	221	54.6	71.4
Don't know	116	28.6	100.0
Total	405	100.0	

*YouTube was banned in Pakistan at the time of survey by the author.

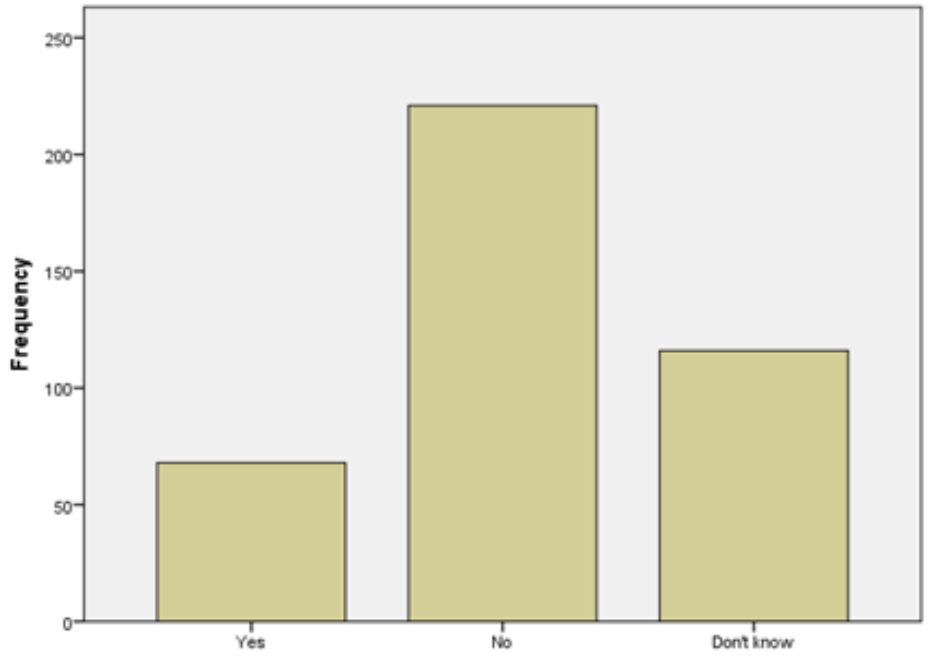

Figure 19: Proxy software usage check graph

Another type of risk which arises due to the children's conduct on the internet is cyber bullying or harassing other children over the internet. Children find that very annoying and disturbing in their way of learning and progress. Cyberbullying is that kind of bullying which is achieved by means of Information & Communication Technology, primarily mobile phones and the Internet. According to research by the author adolescents are using Information & Communication Technology more often hence getting themselves more vulnerable to the risk of being victims of bullying. The results of the survey show that 40% of adolescents used internet every single day. This ratio is high as compared to the ratio of internet usage around the world [7].

Table 33: How often do you use the Internet?

Answer	Occurrence	Percent	Collective Percent
Everyday	162	40.0	40.0
Weekends	51	12.6	52.6
Once a week	52	12.8	65.4
Rarely	140	34.6	100.0
Total	405	100.0	

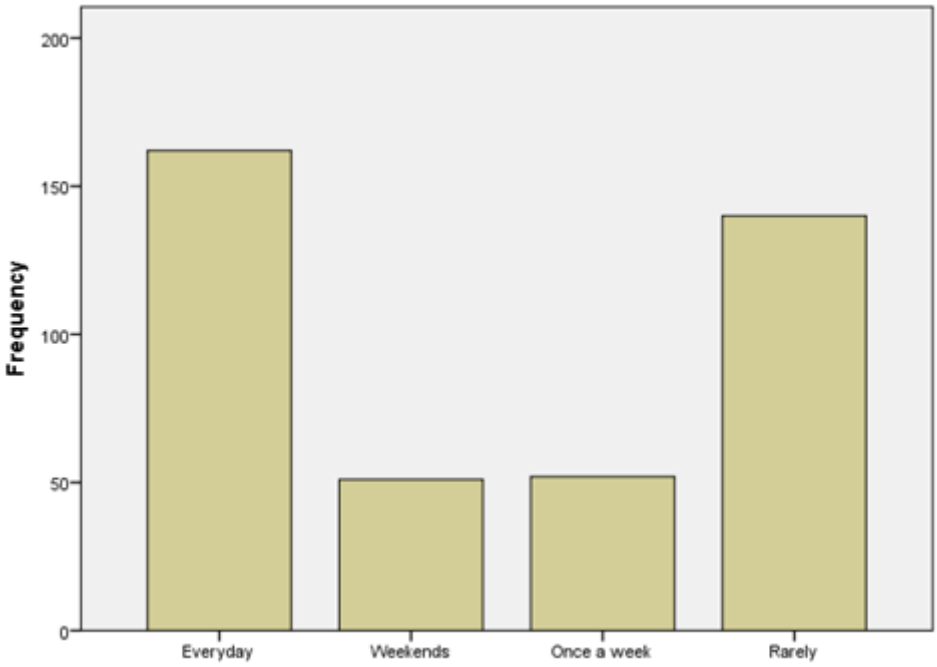

Figure 20: Frequency of usage graph

22% of adolescents in Pakistan have faced cyber bullying by other children which is a high value. When asked by the author what was their response to cyber bullying, 78%

of the victim children replied that they had no idea what to do in response to cyber bullying. The interview of the children by the author revealed that they felt unsafe and scared due to which they did not discuss that with anyone.

Table 34: Have you ever faced Cyber bullying? (Cyber bullying means someone tries to harass or irritate you on the internet deliberately)

Answer	Occurrence	Percent	Collective Percent
Yes	88	21.7	21.7
No	205	50.6	72.3
Don't know	112	27.7	100.0
Total	405	100.0	

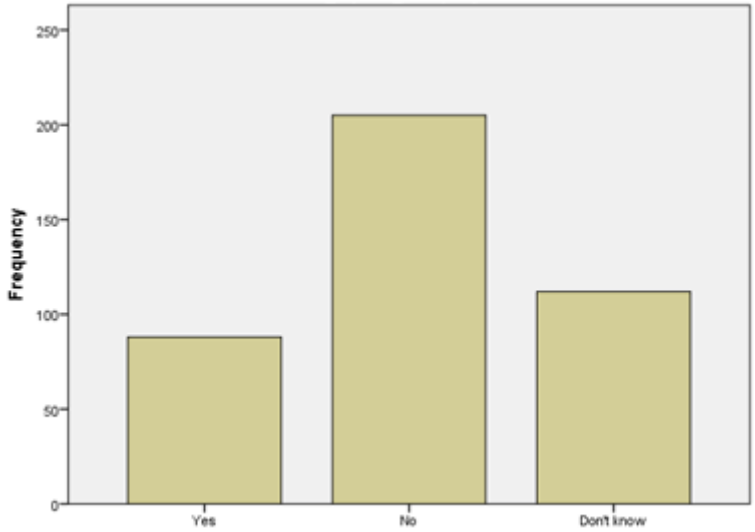

Figure 21: Cyber bullying check graph

Table 35: If yes, what was your response?

Answer	Occurrence	Percent	Collective Percent
No idea what to do	69	78.4	78.4
Told parents	7	8.0	86.4
Told Teacher	3	3.4	89.8
Bullied back	2	2.3	92.0
Ignored	6	6.8	98.9
Got depressed	1	1.1	100.0
Total	88	100.0	

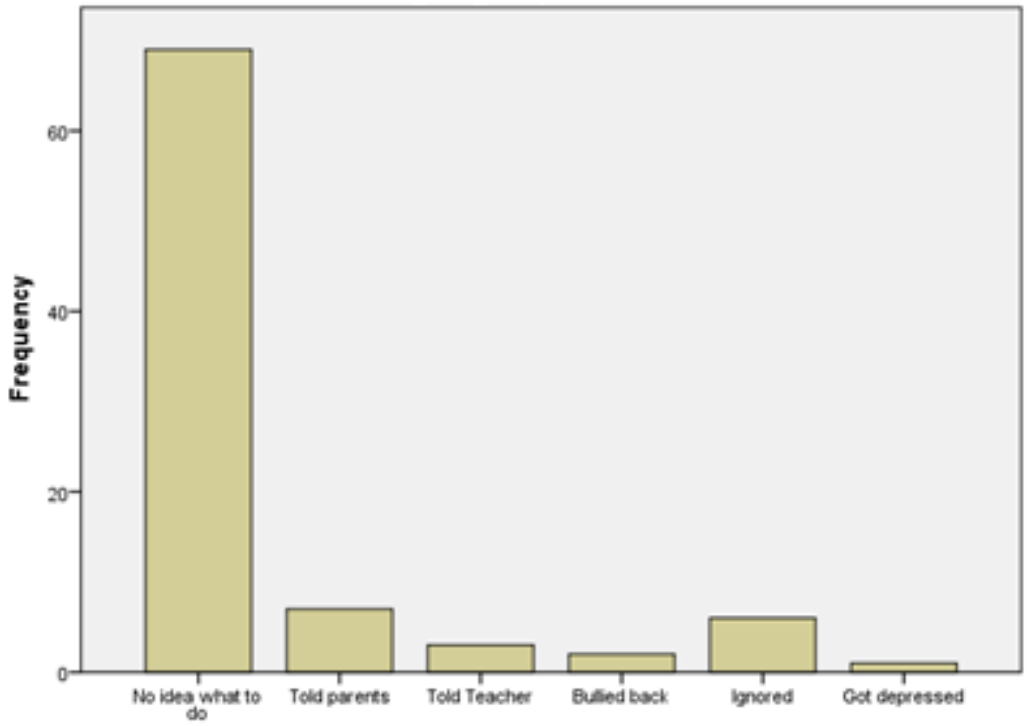

Figure 22: Response to cyber bullying graph

3.4.4 Risks due to low awareness level

There exists a large number of security risks for all internet users globally. According to the author, these risk factors also implement on children. Children are vulnerable to those general user risks which are determined by their own online activities. These general-users' security risks include viruses, spywares, Trojan horses, identity theft, social engineering and phishing. Adolescents are totally unfamiliar about these risks and how the likelihood and impact of these risks can be reduced. During the survey, in response to the question about what potential online risks concerns children the most, 56% of adolescents choose that they do not have any concerns about any risks on the internet.

Table 36: Do you have any concerns going online?

Answer	Occurrence	Percent	Collective Percent
no	226	55.8	55.8
yes	179	44.2	100.0
Total	405	100.0	

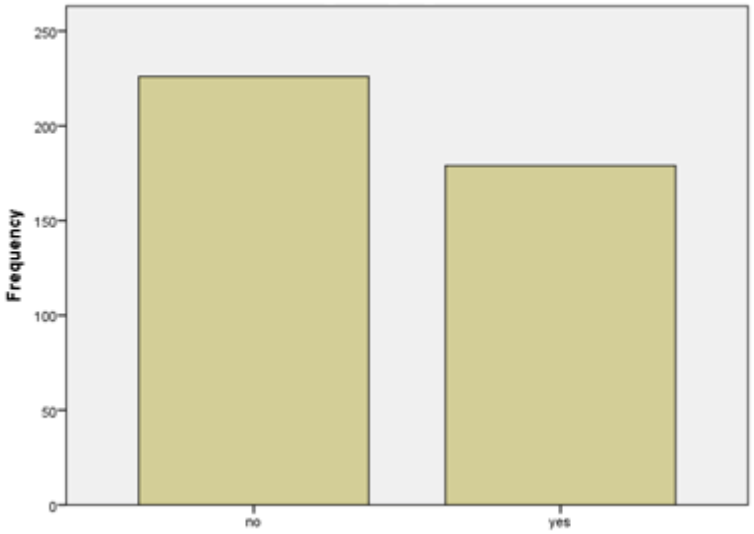

Figure 23: Online risks concern check graph

The level of awareness among secondary school students and higher secondary school students in Pakistan has been found to be low. For many of the questions in the survey to gauge the security awareness level among them, most of the children were found to be unfamiliar with the important terms of information security like confidentiality, integrity, availability, social engineering, spam etc. 88% of children answered that they are unfamiliar with the term integrity including its purpose. 94% have never heard of Botnet, Trojan horse and phishing. 97% have no idea what does encryption means and what are its uses.

Table 37: Are you aware of the term "Integrity" and its purpose?

Answer	Occurrence	Percent	Collective Percent
no	356	87.9	87.9
yes	49	12.1	100.0
Total	405	100.0	

Table 38: Are you aware of the term "Botnet" or "Trojan horse" and its consequences?

Answer	Occurrence	Percent	Collective Percent
no	381	94.1	94.1
yes	24	5.9	100.0
Total	405	100.0	

Table 39: Are you aware of the term "Encryption" and its uses?

Answer	Occurrence	Percent	Collective Percent
No	393	97.0	97.0
Yes	12	3.0	100.0
Total	405	100.0	

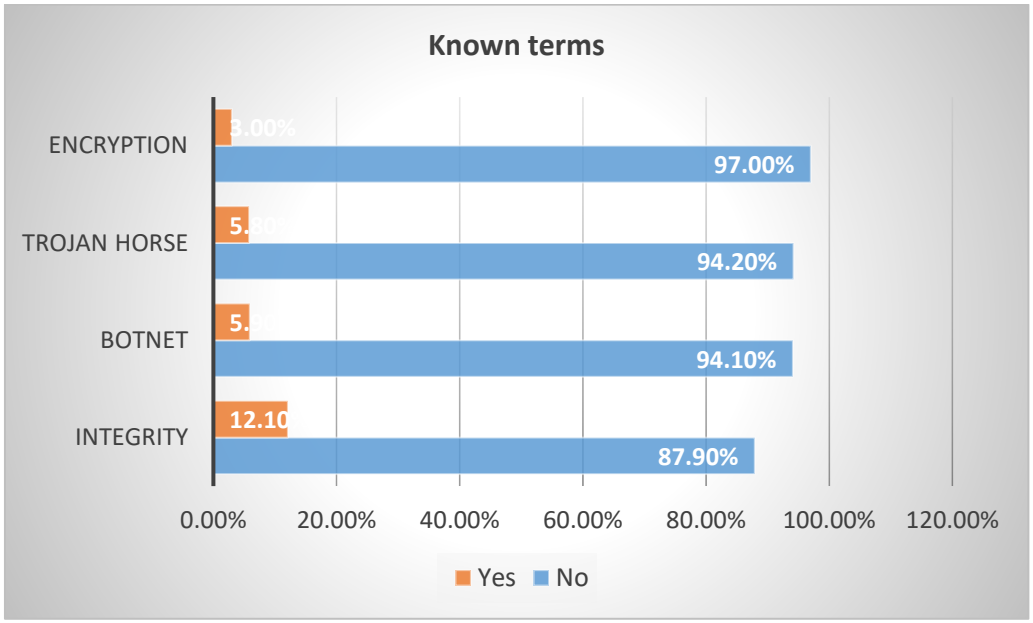

Figure 24: Awareness of security terms graph

3.4.5 Risks, activities and nature of internet usage assessment

After recognizing online risks adolescents are vulnerable to, the type of activities they participate in and the nature of the kid's access to the Internet, Table 36 below represents the assessment of these elements. The activities they participate in will evaluate the sort of risk they are vulnerable to and the nature of their access will gauge the likelihood and their vulnerability to the risk.

Using Table 36, "Risks, activities and nature of internet usage assessment**"** the author presented the risks adolescents may encounter while performing these activities. This is shown in Table 37 below.

Table 40: Risks, activities and nature of internet usage assessment

Risks		Activities leading to vulnerabilities	Nature of internet access increasing the exposure
Contact Risk	Undesirable contact	Excessive Social networking Instant messaging Online gaming	Growth in regularity of access Computer site
	Disclosure of Personal information	Excessive Social networking Instant messaging	Growth in regularity of access Computer site Kid's age
Content Risk	Ambiguous content	Looking up information for schoolwork Browsing topics of interests Internet Surfing for entertainment	Self-learning Growth in regularity of access Computer site
	Lack of age-wise content	Online gaming Browsing topics of interests Internet Surfing for entertainment Looking up information for schoolwork	Growth in regularity of access Self-learning
	Commercialism	Internet Surfing for entertainment Browsing topics of interests Social networking Online gaming	Self-learning Kid's age Growth in regularity of access
Conduct Risk	Illegal downloads	Downloading pictures/audios/videos	Growth in regularity of access Kid's age
	Cyber bullying or harassing	Instant messaging Excessive Social networking	Computer site Growth in regularity of access
	Posting hurtful material	Social networking	Computer site Growth in regularity of access

Table 41: Risks to adolescents based on their activities

Activities	Contact Risks	Content Risks	Conduct Risks
Looking up information and internet surfing for entertainment		Ambiguous content Lack of age-wise content pornography, racist content, hurtful content Commercialism Promotional, advertisement schemes Security Ransomwares, Trojans, spywares	Disclosure of Personal information phishing, identity theft
Social Networking and Instant Messaging	Undesirable contact Strangers/Criminals, Friends, Self Disclosure of Personal information phishing, identity theft	Lack of age-wise content pornography, racist content, hurtful content Ambiguous content	Cyber bullying or harassing Disclosure of Personal information phishing, identity theft
Downloading		Lack of age-wise content pornography, racist content, hurtful content Security Ransomwares, Trojans, spywares	Illegal downloading
Online gaming	Undesirable contact Strangers/Criminals, Friends, Self	Lack of age-wise content pornography, racist content, hurtful content Commercialism Promotional, advertisement schemes Disclosure of Personal information phishing, identity theft Security Ransomwares, Trojans, spywares	Disclosure of Personal information phishing, identity theft Cyber bullying or harassing
Sharing information (Email etc.)	Undesirable contact Strangers/Criminals, Friends, Self	Commercialism Promotional, advertisement schemes	Disclosure of Personal information phishing, identity theft Cyber bullying or harassing

3.5 Risk Management

The extensive variety of risks outlined in Section 3.3 offers parents, educators and policy makers with a tough job to assist and help adolescents handle these risks appropriately. Although adolescents are tech-savvy and possesses the ability to use information and communications technology more resourcefully in contrast to their parents, when it comes to online risks, they are believed to be exposed to destructive content and contacts accessible easily over the Internet [42].

It is undoubtedly concluded that producing a risk-free online environment for adolescents is not possible in any case. A solution to assist adolescents handle these online threats and to support parents become more self-confident at protecting their children against these threats can be originated by means of a risk management approach.

Risk management is the process of falling risks into an acceptable level. Risk management can be categorized into four options; accept, reduce, transfer, and avoid.

i. Risk transfer is defined in ISO/IEC 27005:2011 as *"sharing with another party the burden of loss, or benefit of gain, for a risk"* [43].

ii. Risk acceptance is defined as the *"decision to accept a risk"* [43]. Any of these methods are not applicable in dealing online risks for adolescents.

iii. Risk avoidance is *"the decision not to be involved in, or action to withdraw from a risk situation"* [43]. This supposes that we would forbid adolescents from accessing the Internet. Nevertheless, this way for handling online risks is not practical. Safeguarding adolescents by prohibiting internet usage will restrict kids from availing several online opportunities that the Internet offers. Avoiding risk is also discouraged by various teachers and psychologists, as they realize the requirement for a kid to deal with risks in order to gain their whole potential. Risk is extremely vital for a kid's growth.

iv. Risk reduction is *"the action taken to lessen the probability, negative consequences, or both, associated with risk*" [43]. This can be accomplished through correction, elimination, deterrence, discovery, recovery, and awareness actions. This method has been used more often to help kids handle risks online. Traditionally their

vulnerability to risks has been tried to reduce by means of technical controls. This usually outcomes in restricting kids' opportunities. Age confirmation tools, parental monitoring and social networking sites for children-only are few ways to achieve this. Nevertheless, study has shown that adolescents can bypass these controls [3]. Also, it restricts their opportunities and still leaves children exposed to risks whose parents are not familiar to these controls. A more effective solution is required.

A cyber security awareness program targeting explicitly the adolescents (aged 12-18 years) can achieve the goal. It will encourage kids to adopt appropriate behavior for safe surfing on internet and will encourage them to promote good safety practices. Its goal will be to make kids not only attentive to the risks they face, but also educate them about the safety precautions they can utilize to defend themselves.

3.6 Conclusion

This chapter examined the present study on the threats and hazards adolescents encounter on the Internet. A classification of such risks with an explanation and reasoning of each type was offered and the adolescents' online interests and nature of internet access outlined. A risk management method was used to provide a solution to empower adolescents handle these online threats and to support parents become more self-confident at protecting their children against these risks. The author determined that in order to permit adolescents gain complete advantages of the Internet and practice a harmless online experience, the most useful way is to develop and implement a security awareness programme. These programs make sure that young people have the tools in place and adopt the behaviors that can protect them. The programme will enable them to turn out to be responsible users and offer them the expertise they will require to handle with the risks they may face while surfing the internet.

Chapter 4

CYBER SECURITY AWARENESS CONCEPTS

4.1 Introduction

In Chapter Three, risks effecting adolescents using the Internet were determined. A solution was suggested that to provide protection to children from these risks, an awareness programme on security for adolescents is essential. This chapter observes security awareness concept and how it relates in context of adolescents. Section 4.2 presents a common interpretation of security awareness term and identifies several associated issues. Section 4.3 studies different methodologies for the development of a security awareness programme which are currently in use. Security awareness is then examined in terms of children in Section 4.4 and the development of a programme for children is presented in section 4.5.

4.2 Security awareness programme

4.2.1 Definitions and concepts

As per the definition by Oxford English dictionary [44], awareness is,

> *"Concern about and well-informed interest in a particular situation or development."*

And aware is described as:

> *"Having knowledge or perception of a situation or fact."*

From these definitions, it can be determined that the term security awareness establishes the need for knowing about security. But the idea is far more stronger than this. Information Security Forum's Standard of Good Practice for information security [45] defines security awareness as:

> "*the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization and their individual security responsibilities, and acts accordingly.*"

This concludes that security awareness not only relates to the information only about security concerns but also to act or react based on that information.

For the purpose of increasing awareness level about information security, a security awareness programme shall be developed and executed [46]. A programme is defined in Oxford dictionary as:

> *"a planned, coordinated group of activities, procedures, etc., often for a specific purpose, or a facility offering such a series of activities."*

A security awareness programme is defined in [45] as a

> *"continuous undertaking aimed at building and sustaining a security-positive environment."*

Hence a security awareness programme can be defined as a set of events and procedures that are carried out on defined intervals on regular basis to establish and sustain a proactive security posture.

The National Institute of Standards and Technology (NIST) Special Publication (SP 800-50), "Building an Information security awareness programme" [15], describes a security awareness programme to be effective that is able to,

> "*explains proper rules of behavior for the use of agency IT systems and information."*

Therefore, a security awareness programme is required to be a regular practice to achieve effectiveness, which is helpful to the organization. It shall educate employees about acceptable conduct and activities in such a way that they will realize the importance of security for both of them and the organization.

4.2.2 Standards

ISO/IEC 27001:2013 [17] is the international standard that describes best practice for an Information Security Management System (ISMS). One of the requirements in the standard is the execution of Information Security Trainings and Awareness Programmes [clause 7.2.2.]. It enforces that the organization shall make sure that,

"all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives."

ISO/IEC 27002:2013 [17] is the international standard that establishes controls objectives and controls for Information Security Management System. It defines outline on 144 security controls that shall be established and applied to comply with the requirements of ISO/IEC 27001/2013. Clause 7.2.2 states that

"All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function"

These standards identify the necessity and significance of security awareness education and training and recognize it as an essential feature of an effective Information Security Management System.

4.2.3 Benefits

The benefits of implementing an effective security awareness programme are well documented. The fundamental aspiration of Information Security Awareness is to make participants adopt safe computing practices [47]. The aim of security awareness is to change behavior and reinforce good security practice [47]. An effective security awareness programme will help create and maintain security-positive behavior. It will reinforce the goals of the organization and will ensure that the important messages will get to those who need them [48] [Ch. 12 pg. 200]. An effective programme will enable the participants to understand the relevance of information security for them and how it can help them [48] [Ch. 12 pg. 197]. It will remind the participants not only of the risks they face but the countermeasures they can utilize to guard against them [48] [Ch 43 pg. 522]. SANS technology institute **(SysAdmin, Audit, Network, Security)** [49] state that,

"*security awareness is an effective strategy to reduce the overall risk for an organization. The more users are aware, the greater the chance their behavior will be different, resulting in fewer negative incidents*."

4.2.4 Difficulties

Establishing a successful security awareness programme can be a tough job. There will always be hitches and hindrances to pass. The difficulties described below have been recognized as those which hinder the success of a security awareness programme.

a. *Lack of following up*

Various security awareness programmes have been failed due to failure to follow-up. Consistency is critical for achieving an influential information security programme. Security awareness shall be a regular practice and it is essential that the programme remains active and dynamic. Continuous engagement with the audience is vital to recall them the desired output and updated to the recent security issues.

b. *Lack of considering the audience*

Those security awareness programmes which are intended without specifying the audience will not be as effective as they could be. The targeted material and methods of the programme shall be related to the audience, else the information will not be acknowledged.

c. *Lack of explanation*

One more cause of an ineffective security awareness programme is because of the fact that the awareness programme lacks to describe the reasoning and justification for applying security controls. Users who do not recognize the requirements of certain security behaviors and measures are more unlikely to comply.

d. *Lack of a suitable approach*

In pursuance of an effective information security awareness programme, the approach adopted shall concentrate on behavioral change. Over the period of time, users shall have accepted incorrect manners and in order to change their behaviors it is not sufficient to provide them with related knowledge. Programmes shall identify confrontation to change and utilize a method that will encourage behavior transformation.

e. *Lack of administration support*

Such security programmes shall not prosper and achieve goals which are not embraced by senior management. This is one of the most decisive factor of an effective security awareness programme.

4.3 Security awareness for children

4.3.1 Definitions and Concepts

It is important to define what security awareness means in terms of children. As this has not been documented before the opinions expressed here are those of the author.

By defining what security awareness means for children in terms of the ISF definition [see section 4.2.1], it is the degree to which every child understands the importance of information security and their responsibilities in achieving it, and based on this understanding, they are aware of and execute the appropriate actions. Using NIST's definition [15] of an effective security awareness programme as stated in section 4.2.1, a security awareness programme for children will explain the proper rules of behavior for using IT systems and information. Security awareness programmes are designed to change children's current behaviors and highlight good security habits.

Using the definition outlined in section 4.2.1 [45], an effective security awareness programme for children can be described as a planned, meaningful learning process which will explain the proper rules of behavior for using IT and information.

4.3.2 Standards

There are no international standards for children that advocate explicitly the need for security awareness and training. However, the draft Digital Pakistan policy 2017 [12] by Ministry of Information Technology in Pakistan contains closely related objectives.

4.3.3 Benefits

A number of the benefits of implementing an effective security awareness programme as outlined in section 4.2.3 are also applicable to security programmes for children. They will make children adopt safe computing practices and will change behavior and promote good security practice. The children will understand the relevance of information security and how it can help them. A good security programme will aim to make children aware not only of the risks they face, but also of the countermeasures they can utilize to protect themselves.

According to the **SANS Institute (SysAdmin, Audit, Network, Security)** [49] "*security awareness training is an effective strategy to reduce the overall risk for an organization. The more users are aware, the greater the chance their behavior will be*

different, resulting in fewer negative incidents." In applying this statement to children, one could conclude that the more children are aware, the greater chance their behavior will be different which in turn will result in a smaller number of security incidents involving children.

4.3.4 Difficulties

The difficulties outlined in section 4.2.4 will also apply when developing a security awareness programme for children.

4.4 Establishing an information security awareness programme

4.4.1 Security awareness programme approaches

The paper, **A Design Theory for Information Security Awareness** [50], recognized various approaches to security awareness that have been developed in the past. The list consists of 59 approaches that can be categorized as either cognitive or behavioral with 15 of the mentioned approaches apply both. The paper describes a cognitive method to information security awareness as which objective is to modify user behavior by means of convincing communication. It defines why compliance to acceptable behavior is essential and claims that conducts and actions will not be modified until the information is realized as obligatory in an understandable manner. This can be accomplished by bringing rewards for users who observe an appropriate behavior and conduct as per the information security requirements, and actions against those who deliberately fail to follow the rules. The author of this paper has selected to emphasis on cognitive approaches as he believes that this method encourages lasting modification in behaviors which is mandatory for an effective security awareness programme.

4.4.2 Cognitive approaches

"Building an Information Technology Security Awareness and Training Program" [15] issued by NIST, provides guidance for building an effective information technology security program. The guidance is presented in the form of a life-cycle approach. Consequently, the document puts forward four critical steps in the life cycle of an IT security awareness and training program. (1) Awareness and training program design, (2) awareness and training material development, (3) program implementation and (4) post-implementation. The document offers guidance on (a) identifying training needs, (b) developing a training plan, (c) obtaining funding to the training program, (d) selecting training topics, (e) finding sources of training material,

(f) implementing training material using a variety of methods, (g) evaluating the effectiveness of the program and (h) updating and improving the focus of the program. The publication proposes three different models for an awareness and training programme;

- *Central Program Management Approach* allocates complete responsibilities of the programme to a centralized committee. This centralized committee performs needs assessment to analyze the requirements. It also develops the programme design and learning material. This approach is normally applied in smaller organizations that have same goals throughout the governing board.
- *Partially Central Program Management Approach* assigns the security awareness strategy policy to a centralized penal with operations allocated to line supervisors. Each line supervisor is liable for collection of programme material. This approach is beneficial in larger organization where different departments of the organization have dissimilar requirements.
- *Distributed Program Management Approach* distributes the information security policy and requirements on awareness and training. A separate programme is planned, established and conducted by each department of the organization. This approach is useful in large organizations where each department has miscellaneous goals.

Figure 35 shows the model proposed by the **Information Security Forum** [45] for developing a security awareness programme. This is a four-step model that results in the design of numerous campaigns which can run side by side or in succession. Each campaign has a distinct design, development and delivery stage.

• Stage One – Objectives and goals are identified based on the problems to be solved. A risk assessment approach is suggested as a method to help define objectives for the programme as it provides a thorough, reliable approach for analyzing the problems and identifying objectives to manage those problems.

• Stage Two – The scope and design of the programme is defined. An important aspect of this stage is preparing to change behavior using Lewin's process of force field analysis [51].

• Stage Three – Security and awareness campaigns are developed and implemented.

• Stage Four – The effectiveness of the campaigns is measured.

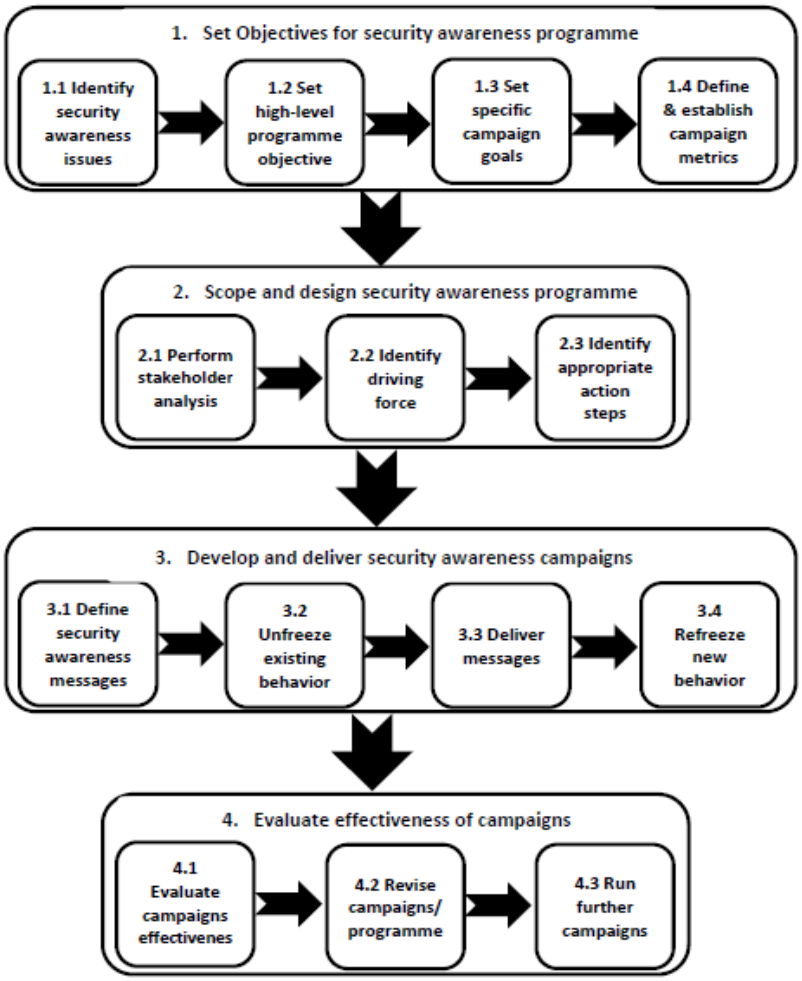

Figure 25: ISF for effective security awareness

4.5 Conclusion

In this chapter, a definition of security awareness and a security awareness programme was introduced. This was followed by the identification of the standards, benefits and difficulties of security awareness programmes. The author then applied this theory to create a definition of security awareness and security awareness programmes for children. The components, benefits and difficulties of such a programme for children were discussed.

Guidelines for developing a security awareness programme for children have not yet been developed. Utilizing the approaches described in section 4.3.2 and making

appropriate changes to the processes and sub-processes the subsequent chapter presents guidelines for preparing and implementing an information security awareness programme that is suitable for use at school level.

Chapter 5

CYBER SECURITY AWARENESS PROGRAMME

5.1 Introduction

Chapter Four outlines the standards, benefits and difficulties associated with developing a security awareness programme for adolescents. This chapter utilizes the information and presents guidelines on how to develop such a programme for use in an educational institute. It also outlines the details of the development of a security awareness programme for children aged between twelve and eighteen, the target audience of the author's own study. This is highlighted in italics throughout the chapter. Section 5.2 identifies the necessary processes for designing, planning, and assessing the programme. Section 5.3 describes how to execute and manage the programme followed by evaluation and assessment guidelines in section 5.4.

5.2 Phase One: Strategy, design and plan

The first phase in the development of an awareness programs includes the identification of the awareness needs of the students in a school, followed by development of an awareness plan and gets the consent of principal, educators and other associates of the school community.

5.2.1 Initiating a Programme Committee

As stated above in Section 4.4.2., there are several methods to design, develop and implement an awareness programme. According to this author the best appropriate approach in the development of an awareness programme in a school atmosphere is through a centralized program. This approach allocates the job for developing and implementing the cyber security awareness programme to a committee. This committee is the stirring power behind the programme whose goal is to check that the plan is implementing. The memberships of the committee must be subjected to the devotion to the job as the effectiveness of the awareness programme shall be determined by the efforts they spend in the development of plan and implementation. Appropriate members of this committee are the school principal, educators and skillful parents.

The author will perform as the programme committee for the resolutions of developing and implementing the awareness programme proposed in this study.

5.2.2 Measuring the requirements of the audience

Awareness programs shall be planned and created explicitly for the spectators they are aiming [46]. This is an important factor in the successful implementation of the programme [Section 4.2.4]. In a school, different groups can be targeted for an awareness programme including the students, the parents, teachers, the lab assistants and other school staff. The requirements of each target group will be dissimilar and different means of communication will be needed in order to approach each group efficiently. Each of the selected group shall be assessed and the security threats that they may encounter them identified. There will be few intersection areas among groups but vulnerability to the risk for each target group will not be the same so as the content and distribution mechanism [15]. It is critical to study the skill level and knowledge of each group separately. This study should contain their Internet usage routines and online activities, their level of awareness about cyber security hitches and their level of awareness about protective actions to counter them. The study can be accomplished by conducting a survey and it will make sure that the content in the awareness programme is designed as per the requirements of the audience [15].

The scope of the programme outlined here contains adolescents aged from twelve to eighteen (12-18) years. No research has been made exclusively on this age group to date. The author circulated self-administered need assessment survey questionnaire to all four categories of primary and secondary schools i.e. public, private (local), private (international) and military schools. Afterwards, interviews of half of the respondents were conducted to verify the response and results. Three different surveys were conducted for different target audience; primary school students aged between 12 and 18, parents of these students and their teachers. This survey finalized by 405 Pakistani children, parents and teachers intended to fold evidence on these kids' internet conducts; regularity of access, activities on the internet, awareness about the risk factors and their knowledge of the security measures. Parents were measured to build an overall understanding of their parenting attitudes and conducts concerning their kids' internet access and to find the level of their awareness of few technical security measures. A third survey was conducted to gain information regarding teacher's

interaction of the internet with adolescents and to determine their knowledge of current children internet safety initiatives.

The results of the survey identified that the most widespread activities that kids participate in over the internet are looking up information for schoolwork (54.3% n=405), social networking (Facebook, Twitter etc.) (49.4% n=405), downloading pictures/audios/videos (37% n=405), online gaming (30% n=405), sharing pictures and information (25.7% n=405), surfing/browsing web pages (25% n=405), and communications (email, instant messaging etc.) (20% n=405).Using Table 36, "Risks, activities and nature of internet usage assessment" the author presented the risks adolescents may encounter while performing these activities. This is shown in Table 37 above.

Almost half of the sample respondents declaring that they have educated themselves at their own how to access and use the internet for various purposes (47.7%). School teacher was the second most basis for learning to use the Internet (20.7%) followed by siblings (14.8%).

The level of awareness among secondary school students and higher secondary school students in Pakistan has been found to be low. For many of the questions in the survey to gauge the security awareness level among them, most of the children were found to be unfamiliar with the important terms of information security like confidentiality, integrity, availability, social engineering, spam etc. 88% of children answered that they are unfamiliar with the term integrity including its purpose. 94% have never heard of Botnet, Trojan horse and phishing. 97% have no idea what does encryption means and what are its uses. In response to the question about what potential online risks concerns children the most, 56% of adolescents choose that they do not have any concerns about any risks on the internet. All this specifies a lack of awareness of their own competence to handle the risks. The results of this survey establish the fact that overall adolescents in this target group do not possess acceptable education and knowledge of the related risks and safety measures.

5.2.3 Identifying programme objectives

The most critical factor in the establishment of an effective awareness programme is the identification of well-defined objectives [46]. The guidelines specified by the ISF

Model in section 4.4.2 can be applied to outline the objectives for creating a security awareness programme.

a. Categorize issues that will be addressed by a security awareness programme.
b. Identify high level programme objectives for the problem categorized earlier.
c. Establish definite programme goals to set the purpose of each campaign.
d. Define and establish campaign metrics so that the success of the campaign can be measured.

These campaigns address the risk that adolescents are regular Internet users but do not hold the required expertise and knowledge to handle the risks effectively. The survey shows that 40% of adolescents used internet every single day. The results of the survey also discovered that adolescents are unfamiliar with most of the cyber security risks they may encounter online and of proper safety controls.

The aim of the security awareness programme is to empower adolescents with the basic knowledge and skill about the risks they may encounter online and conduct a responsible and safer user behavior to safeguard themselves. After evaluating the activities adolescents participate in with respect to the related risks, the author identifies three areas of concern which are: security, safety, and web browsing skills. Separate campaigns shall be directing each of these areas.

Cybercampaign one - Security
This cybercampaign will explain to the adolescents the possible measures and controls to protect their usage sessions online and teach them about best password practices, protection from botnets, spyware, social engineering, phishing, spam and unfamiliar emails.
In result of the programme the kid will be able to: • *Recognize the best practices for password creation, protection and change.* • *Realize the terms Confidentiality, Integrity and Availability and their purposes.* • *Outline the terms spyware, spam, social engineering, trojans and cyber bullying and adopt the security measures to safeguard themselves from these risks.* • *Differentiate between personal information what can be shared on the internet including social networking websites and what should be kept private.*

- *Understand the proper process to handle issues like email messages including attachments from unfamiliar sources, phishing and free downloads.*

Cybercampaign two - Safety
The purpose of this cybercampaign is to prepare adolescents as a skilled and expert user of the internet so that they will be able to protect themselves from this wide range of cyber threats. The topics covered will be about undesired contacts from strangers/criminals, cyber bullying and acceptable online behavior also known as cyber ethics.
In result of the programme the kid will be able to: • *Summarize critical Internet safety rules and procedures.* • *Describe the term cyberbullying and adopt adequate practices to handle it.* • *Enlighten the importance of retaining personal data private.* • *Demonstrate safe communication through messaging and chat with friends and family.* • *Understand and adopt online best practices for acceptable conduct on the internet.*

Cybercampaign three – Web browsing skills
The purpose of the web browsing skills cybercampaign is to empower adolescents with elementary safe browsing concepts and offer them the required skill level to differentiate between several kinds of information they may find on the internet.
In result of the programme the kid will be able to: • *Identify secure search engines and appropriate techniques to improve searches.* • *Differentiate between legitimate and fake websites for information gathering.* • *Utilize the bookmarking options to save their favorite websites for further exploration.* • *Assess and evaluate information found on the Internet together with the marketing and advertising content.* • *Perform actions to take if they face content that is inappropriate and disturbing for them.*

5.2.4 Selecting appropriate source content for the programme

The content and resources for the awareness programme shall be selected carefully. There is a varied range of teaching resources on cyber security awareness topics for

children offered on the Internet through various cyber security awareness programs. Many governmental organizations also developed appropriate resources for primary and secondary schools. Guidance and material may also be collected from other institutes that have already implemented an awareness programme.

A comparison of numerous cyber security awareness programs for children around the world has been made in Table 1 to recognize the purpose of each resource and what topics and resources each program offer. The content of these resources could be utilized by parents and teachers for educational purpose and also as a source material suitable for the awareness programme.

The author has also developed appropriate resource material as per the objectives of the campaigns outlined above. Each campaign has different set of resources to be opted and used by schools to teach adolescents about cyber security. The content of the resources has been carefully developed considering the risks identified in chapter 3 and also the activities and interests of the adolescents on the interent. The resource material can be utilized both individually by adolescents or by a group of students and is available online [52]. *A few samples of resource material are provided in Appendix-D.*

5.2.5 Choosing suitable approach

Chapter 4 section 4.2.4 recognized the problems that shall be mitigated for the effective development and implementation of an awareness programme. Absence of a suitable approach was one such difficulty declared above. The goal of an awareness programme is to alter users' behavior and conduct. For the achievement of this, the awareness programme shall take into account a behavioral change management approach [46]. In an educational institution, this method can be reached through specific coaching procedures and counselling techniques. Ideology and inclination of a person play an important role in the behavior and conduct by that person. Altering behavior is a difficult task and teachers shall adopt teaching techniques that effectively addresses kids' previous theories and ideology.

This type of teaching is known as conceptual transformation. It consists of a procedure to consider adolescents' presumptions and inspiring them to revive their assumptions according to the recent information established. This procedure of pedagogy is very effective only if adolescents receive the new material realistic, logical and productive.

It includes a four-step procedure. (1) identify adolescent presumptions, (2) discuss and analyze presumptions, (3) create theoretic disagreement with those presumptions, (4) inspire and educate conceptual rebuilding.

A successful security awareness programme shall be intended to consider the fact that during the presentation sessions, the focus of the attendants decreases with the passage of time. The presentations shall therefore be imaginative, attractive and encouraging focusing primarily to seek attention of the attendant in order to include the learning in sensible decision-making.

5.2.6 Selecting mode of distribution

The next step in the planning of the awareness program is to choose the right mode of distribution of content to target audience. A security awareness programme can be treated as a promotion campaign. The first step is to know client requirements through need assessment, the next step is to choose the items, adjust it as per requirements of the client and at last package it appealingly. By communicating the right content to the target audience, using the most attractive distribution method the target audience will show full concentration and they will be highly motivated to absorb the objectives of the programme.

The mode of distribution of cyber security awareness programme consists of tip sheets, posters, activity sheets, leaflets, games and quizzes.

5.2.7 Designing the awareness programme

A complete range of areas to be included in the awareness programme shall be listed and the objectives, material and distribution mode for each area shall be identified.

The author expresses his opinion that this part of the awareness programme shall be conducted by each class teacher. As concluded in section 5.2.6 the source material of the awareness programme must be delivered attractively and explicitly as per the requirements of the target audience. This can be achieved by applying ideal learning styles. Each class tutor will possess adequate expertise about this and will select from the provided material an acceptable mode of distribution.

5.3 Phase Two: Implement and Manage

Following the collection of suitable material and identifying a plan it is time to implement the awareness programme and achieve the objectives and purposes established earlier. A detailed description of each plan activity and objectives shall be provided to all the workforce associates who will be communicating the resources. They shall clearly realize their definite part and responsibilities for implementing the programme.

As stated in section 4.2.4, steadiness is an important factor to a successful awareness programme and continuous involvement is critical in order to retain the programme for better results. After the programme plan is initiated, consistent repetition of the content is vital to recall the target audience of the key messages and to place security risks and threats visible to them at all times.

In case of a school or college, implementation of the awareness programme will be a continuous process lasting over the academic year with educators teaching the benefits and threats of the cyber world but in order to achieve rapid effectiveness, it is also necessary to communicate the key areas of concern to the audience at different times. There exist numerous initiatives around the world that schools and colleges can endorse to attain this like Computer security day on November 30 and Safer internet day on February 6, etc. These initiatives can help raise the awareness about specific security concerns and can promote safer and responsible use of the internet. The school or college can also arrange a security week where a targeted set of events and activities can occur.

5.4 Phase Three: Assess and restructure

In order to assess the achievements of the awareness programme and to evaluate its performance, review of the audience is needed. The feedback can be obtained via evaluation forms, user acceptance testing and teacher observations etc. The results of the feedback shall be evaluated and the improvements shall be used to restructure the programme as required.

In order to evaluate programme achievements and success, it is the opinion of the author to re-conduct the same questionnaire and interviews with adolescents to analyze their understanding and knowledge about the delivered areas of concern.

5.5 Conclusion

This chapter applied the information concluded earlier in the prior chapters to deliver a set of plans and procedures for the development of an internet security and safety awareness programme to be implemented in a secondary or higher secondary school. Section 5.2 sets outline on proposed procedures to follow in the development of the programme. Guidelines on implementing and managing the programme are proposed in section 5.3 and section 5.4 recommends measures to evaluate the effectiveness of the awareness programme.

The participant schools in the survey have shown strong interest in executing the final programme as soon as the new academic year starts next year.

Bibliography

[1] D. Pruitt-Mentle, "Educational Technology Standards and Performance Indicators for Students," ikeepsafe, 2000. [Online]. Available: http://www.ikeepsafe.org/educators_old/more/c3-matrix/. [Accessed 2017].

[2] M. Ribble, "Digital Citizenship using Technology appropriately," International Society for Technology in Eduction, 2017. [Online]. Available: http://www.digitalcitizenship.net/. [Accessed 2017].

[3] "Eu Kids Online - Findings. methods. recommendations," London School of Economics & Political Science, London, 2014.

[4] L. S. P. Partow-Navid, "Students Information Security Practices and Awareness," *Journal of Information Privacy and Security* , vol. 8, no. 4, pp. 3-26, 2014.

[5] M. Padric, "An investigation of online threat awareness and behavior pattern amongst secondary school learners," 2012.

[6] UNICEF, "Statistics," UNICEF, 2015. [Online]. Available: https://www.unicef.org/infobycountry/pakistan_pakistan_statistics.html. [Accessed 2017].

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

[8] "https://www.ibm.com/analytics/us/en/technology/spss/," IBM. [Online]. [Accessed 2017].

[9] A. B. e. al., "Introducing IT- security Awareness in schools: the Greek Case," in *First World Conf. on Info. Sec. Education*, Carolina, 1999.

[10] C. E. I. S.-K. C. D. Frincke, "Integrating Security into the Curriculum," *Computer*, vol. 31, no. 12, pp. 25-30, 1998.

[11] N. A. Secretariat, "Prevention of Electronic Crimes Act," 22 August 2016. [Online]. Available: http://www.na.gov.pk/uploads/documents/1472635250_246.pdf. [Accessed 2017].

[12] M. o. InformationTechnology, "Digital Pakistan Policy 2017," 2017. [Online]. Available: http://moit.gov.pk/policies/DPP-2017v5.pdf. [Accessed 2017].

[13] M. o. I. Technology, "National IT Policy 2016," March 2016. [Online]. Available: http://moit.gov.pk/policies/National_IT_Policy_2016.pdf. [Accessed 2017].

[14] M. o. Education, "National curriculum for Computer Education for Grades VI-VIII," 2007. [Online]. Available: http://pctb.punjab.gov.pk/system/files/Computer%20Education%20VI-VIII.pdf. [Accessed 2017].

[15] N. I. o. S. a. Technology, "Building an Information Technology Security Awareness and Training Program," October 2003. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. [Accessed 2017].

[16] N. I. o. S. a. Technology, "A role-Based Model for Federal Information Technology/Cyber Security Training," 1998. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf. [Accessed 2017].

[17] I. O. f. Standardization, "Information technology - Security techniques - Information security management systems - Requirements," 2013. [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed 2017].

[18] S. -. H. S. a. G. Affairs, "Federal Information Security Modernization Act of 2014," 2014. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/2521. [Accessed 2017].

[19] E. O. o. t. P. (US), "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," 2009. [Online]. Available: https://www.dhs.gov/sites/default/files/.../Cyberspace_Policy_Review_final_0.pdf. [Accessed 2017].

[20] E. Union, "General Data Protection Regulation," 2016. [Online]. Available: ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. [Accessed 2017].

[21] "Cyber Safe," Cyber Security Malaysia, 2017. [Online]. Available: http://www.cybersafe.my/en/. [Accessed 2017].

[22] "Secure Verify Connect," BRUCERT, 2017. [Online]. Available: www.secureverifyconnect.info/. [Accessed 2017].

[23] "Go Safe Online," Cyber Security Awareness Alliance, 2017. [Online]. Available: https://www.csa.gov.sg/gosafeonline/. [Accessed 2017].

[24] "CYBER WELLNESS," Ministry of Education, Singapore, 2017. [Online]. Available: https://www.moe.gov.sg/education/programmes/social-and-emotional-learning/cyber-wellness. [Accessed 2017].

[25] "Savvy Cyber Kids," Savvy Cyber Kids Inc., 2017. [Online]. Available: http://savvycyberkids.org/. [Accessed 2017].

[26] "Digizen," ChildNet International, 2017. [Online]. Available: http://www.digizen.org/. [Accessed 2017].

[27] "Security Awareness," RSA, 2017. [Online]. Available: https://community.rsa.com/docs/DOC-40434. [Accessed 2017].

[28] "Webwise," Co-Financed by the European Union with various organizations, 2017. [Online]. Available: https://www.webwise.ie/. [Accessed 2017].

[29] "Think U Know," CEOP Child Exploitation and Online Protection Centre, 2014. [Online]. Available: https://www.thinkuknow.co.uk/. [Accessed 2017].

[30] "Hacker High School - Security Awareness for Teens," ISECOM, 2017. [Online]. Available: www.hackerhighschool.org/. [Accessed 2017].

[31] "Get Cyber Safe," Governement of Canada, 2017. [Online]. Available: https://www.getcybersafe.gc.ca/index-en.aspx. [Accessed 2017].

[32] "Esafety Information," Office of the Esafety Commissioner Australia, 2017. [Online]. Available: https://esafety.gov.au/. [Accessed 2017].

[33] "Netsmartz," National Center for Missing & Exploited Children, 2017. [Online]. Available: https://www.netsmartz.org/Parents. [Accessed 2017].

[34] "NS TEENS," NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, 2017. [Online]. Available: http://www.nsteens.org/. [Accessed 2017].

[35] "Stay Safe Online," National Cyber Security Alliance, 2017. [Online]. Available: https://staysafeonline.org/. [Accessed 2017].

[36] "Information Security awareness material," European Union Agency for Network and Information Security (ENISA), 2017. [Online]. Available: https://www.enisa.europa.eu/media/multimedia/material. [Accessed 2017].

[37] "Employee Security Awareness Survey," 2017. [Online]. Available: https://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf. [Accessed 2017].

[38] E. Commission, "Safer Internet for Children Qualitative Study in 29," European Commission, 2007.

[39] H. J. Kim, "Online Social Media Networking and Assessing Its Security Risks," *International Journal of Security and Its Applications,* vol. 6, no. 3, pp. 11-18, 2012.

[40] "Company info - Stats," Facebook, June 2017. [Online]. [Accessed 2017].

[41] Microsoft, "The Naked Truth teen Infographic," November 2016. [Online]. Available: go.microsoft.com/?linkid=9781985. [Accessed 7 august 2017].

[42] E. L. S. Staksrud, "CHILDREN AND ONLINE RISK," *Information, Communication & Society* , vol. 12, no. 3, pp. 364-387, 2011.

[43] I. O. f. Standardization, "Information technology -- Security techniques -- Information security risk management," June 2011. [Online]. Available: https://www.iso.org/standard/56742.html. [Accessed 2017].

[44] "English Oxford dictionaries," Oxford University Press, 2017. [Online]. Available: https://en.oxforddictionaries.com/. [Accessed 2017].

[45] I. S. Forum, "Standard of Good Practice For Information Security," June 2014. [Online]. Available: https://www.securityforum.org/uploads/2015/02/Standard-of-Good-Practice-ES-2014_Marketing.pdf. [Accessed August 2017].

[46] ENISA, "The new users' guide: How to raise information security awareness," 29 November 2010. [Online]. Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide. [Accessed August 2017].

[47] Y.-Y. C. Y.-Y. Chan, "Teaching for Conceptual Change in Security Awareness," *IEEE Security & Privacy,* vol. 6, no. 6, pp. 67-69, 2008.

[48] H. K. M. Tipton, Information Security Management Handbook, Auerbach: CRC Press, 2000.

[49] Chelsa Russell, "Security Awareness - Implementing an Effective Strategy," 2002. [Online]. Available: https://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418. [Accessed 2017].

[50] P. Puhakainen, "A Design Theory for Information Security Awareness," Faculty of Science Department of Information Processing Science, Oulu, 2006.

[51] K. Lewin, Resolving social conflicts, New York: Harper, 1945.

[52] "Cyber Security Awareness Programme for Adolescents," 2017. [Online]. Available: http://csirt.nust.edu.pk/index.php/trainings/.

APPENDIX A

Questionnaire for Adolescents

Class: _____ Gender: _____

Age: _____ City: _____

Date: _____ School/College: _____

Section 1 - Usage

Q1. How often do you use the Internet?

☐ Everyday	☐ Weekends only	☐ Once a week
☐ Rarely	☐ Never	☐ Other : _____

Q2. How much time do you spend on the Internet daily?

☐ Half an hour	☐ One hour	☐ Two hours
☐ Four hours	☐ More than five hours	☐ Other : _____

Q3. Where do you access the Internet? (Please tick all relevant boxes)

☐ At home	☐ In an Internet cafe	☐ In a friend's home
☐ At school	☐ In a relative's home	☐ Other : _____

Q4. Which devices do you use to access the Internet? (Please tick all relevant boxes)

☐ Using a mobile/Smart phone	☐ Using a laptop	☐ Using a home PC
☐ Using a tablet	☐ Using a Public Computer	☐ Other : _____

Q5. Which medium do you use to access the Internet? (Please tick all relevant boxes)

☐ Landline Broadband	☐ Wireless broadband (Evo, Witribe, Wingle)	☐ Mobile networks (GPRS, 3G, 4G)
☐ Public Wi-Fi	☐ Dial-up connection	☐ VSAT/Comlink

Q6. How much time do you spend on Facebook daily?

☐ Half an hour	☐ One hour	☐ Two hours
☐ Four hours	☐ More than five hours	☐ Other : _____

Q7. Do you have a mobile phone?

☐ Yes ☐ No

If yes, what do you use it for? (Please tick all relevant boxes)

☐ Making and receiving calls	☐ Text Messaging	☐ Social networking	☐ Listening to music
☐ Taking and uploading pictures	☐ Maps and locations	☐ Downloading/Using apps	☐ Other : _____

Section 2 – Activities

Q8. What do you use the Internet for? (Please tick all relevant boxes)

☐ Online gaming	☐ Looking up information for schoolwork	☐ Downloading pictures/videos/audios
☐ Browsing web pages	☐ Social networking (Facebook, Twitter)	☐ Communication (Email, Instant messaging)
☐ Sharing files	☐ Sharing pictures and information	☐ Other : _____

Q9. What is the greatest benefit the Internet has brought to your life?

☐ Learning	☐ Socializing	☐ Exploring
☐ Entertainment	☐ Contacting	☐ Other : _____

Q10. How many times did you change your password?

☐ Never Changed	☐ Everyday	☐ Once a Week
☐ Once a Month	☐ Once a Year	☐ Never believed its important

Q11. Do you use same password for different accounts?

☐ Yes ☐ No

If yes, for how many accounts? (Please tick all relevant boxes)

☐ Two ☐ Three ☐ Other : _____

Q12. Do you regularly turn off your Wi-Fi and Bluetooth connections after using them?

☐ Yes ☐ No ☐ Don't know

Q13. Do you use location and GPS image services for photo sharing and telling where you are?

☐ Yes ☐ No ☐ Don't know

Q14. Do you use pirated and cracked software on your devices?

☐ Yes ☐ No ☐ Don't know

Q15. Do you use proxies for accessing restricted websites like YouTube?

☐ Yes ☐ No ☐ Don't know

Q16. Who has shown you how to use the Internet?

☐ My parents/guardian	☐ My teacher	☐ Self-learning
☐ My brother/sister	☐ My friends	☐ Websites, blogs

Section 3 – Contact Risk Factor

Q17. What kind of people you are interested to add to your friend list on Social Networking Services (SNS) like Facebook etc?

☐ Someone who looks familiar ☐ People I am sure I know ☐ Anyone, I don't care

Q18. Is your profile private? (A private profile means that only your friends can view your profile)

☐ Yes ☐ No ☐ Don't know

Q19. Do you share you email address or account with strangers?

☐ Yes ☐ No ☐ Don't know

Q20. For which of the following pieces of information would you ask your parent's permission before sharing it on the Internet?

☐ My name	☐ My pet's name	☐ My phone number
☐ My school	☐ My address	☐ My Hair color
☐ My email address	☐ My age	☐ My family details

Q21. Who do you feel is effective at helping you maintain the online security, privacy and safety of your personal information online?

☐ My Self	☐ Online companies	☐ Parents
☐ Government	☐ Schools	☐ Teachers

Q22. Do you think the Internet is a safe place?

☐ Yes ☐ No ☐ Don't know

Section 4 – Content Risk factor

Q23. Tick all the terms that you are aware of? (Please tick all relevant boxes)

☐ Confidentiality	☐ Integrity	☐ Availability	☐ Anti-virus
☐ Virus	☐ Botnet	☐ Social engineering	☐ Firewalls
☐ Trojan horse	☐ Spam	☐ Phishing	☐ Encryption

Q24. Do you believe that the information you find on the Internet is always true and correct?

☐ Yes	☐ No	☐ Don't know

Q25. Have you ever faced Cyber bullying? (Cyber bullying means someone tries to harass or irritate you on the Internet deliberately)

☐ Yes	☐ No	☐ Don't know

If yes, what was your response?

☐ I told my parents	☐ I told my teacher	☐ I bullied back
☐ I ignored it	☐ I got depressed	☐ I had no idea what to do

Q26. Have you ever received threatening calls or messages from someone?

☐ Yes	☐ No	☐ Don't know

Q27. Have you ever been hacked?

☐ Yes	☐ No	☐ Don't know

If yes, what were the consequences?

☐ I lost my password	☐ I got viruses on my computer	☐ I crashed my device
☐ I lost data	☐ I have no idea what happened	☐ My profile was compromised

Section 5 – Conduct Risk factor

Q28. Do you have an email account?

☐ Yes	☐ No

If yes, do you open emails from people you do not know?

☐ Yes	☐ No

Q29. What potential online risks concerns you the most?

☐ Being bullied or harassed online	☐ Loss of personal privacy	☐ Poor performance of computer
☐ Online information damaging relationship with family/friends	☐ Finding viruses, spyware, adware or other tracking software on my devices	☐ I don't have any concerns going online
☐ Data loss	☐ Financial loss	☐ Other : _____

Q30. What's your understanding about illegal downloads? (Movies, Music, Books etc.) Please tick all relevant boxes

☐ Everyone does it	☐ I do it for private use only	☐ It is illegal
☐ It is cheaper	☐ It does contain risk	☐ Don't know

Q31. Which Wireless connection (Wi-fi) you consider safe to join?

☐ Password protected	☐ One I configured myself	☐ I know the SSID
☐ Any open network	☐ Only my home/school network	☐ Don't know

Section 6 – Awareness

Q32. What you believe corresponds best to the risks with **email, instant or text messaging attachments**? (Please tick all relevant boxes)

☐ All attached files are potentially harmful and may contain viruses	☐ If I know and trust the sender I can always open the attachment	☐ Only attached files with the extension .EXE pose a real risk
☐ It is safe to open attachments if I have a firewall installed on the computer	☐ An anti-virus reduces the risk of being infected by viruses from email attachments	☐ Don't know

Q33. Tick what you think is correct about **anti-virus** software and **firewalls.** (Please tick all relevant boxes)

☐ Anti-virus software searches your hard drives for viruses and protects your private network	☐ A firewall protects the resources of a private network from users of other networks	☐ A firewall searches your hard drives for viruses and protects the resources of a private network from outsiders
☐ Anti-virus software searches your hard drives for viruses	☐ Anti-virus software should never be used together with a firewall	☐ Don't know

Q34. Updating/Patching is important because.....

☐ It makes my computer less vulnerable to virus attacks.	☐ It fix problems with a computer program or its supporting data	☐ It reduces spam in my inbox
☐ Patches remove viruses	☐ All of them	☐ Don't know

Q35. What indicates you are browsing a website in **a secure** manner? (Please tick all relevant boxes)

☐ The URL/address of the web site starts with "**https://**"	☐ They are selling quality goods from famous brands	☐ There's a banner on the top of the page saying "Secure Website"
☐ I know the company	☐ All of the above	☐ Don't know

Q36. Tick what you consider is correct about **backing up** data. (Please tick all relevant boxes)

☐ I should only backup photos stored on my computer	☐ Any important information should be backed up	☐ Files I don't want change in the future only have to be backed up once
☐ I should never use CD-RW as external storage	☐ Backup is useless	☐ Don't know

Q37. Tick what you think is correct about **Encryption.** (Please tick all relevant boxes)

☐ Encryption is expensive for home-users	☐ Encrypted files cannot be disclose others	☐ Not all data can be encrypted
☐ E-mails do not have to be encrypted unless sent with attachments	☐ Encryption protects the confidentiality of information	☐ Haven't heard about it before

Q38. Tick what you think is correct about USB flash drives. (Please tick all relevant boxes)

☐ They are not suitable for storing photos	☐ They should be scanned before use	☐ They are expensive in relation to storage capacity
☐ They are easy to misplace or lose	☐ They may contain viruses	☐ Don't know

APPENDIX B

Questionnaire for Parents

Child's Class: _____

Child's Age: _____

Date: _____

Q1. How often does your child use the internet at home?

☐ Once a week	☐ Weekends only	☐ Rarely
☐ Everyday	☐ Never	☐ Other: _____

Q2. Do you have separate user accounts on your home computer/laptop?

☐ Yes	☐ No

Q3. Do you have an anti-virus, anti-spyware or spam-filtering software on your computer/laptop?

☐ Yes	☐ No	☐ Don't know

Q4. Are the parental control features on your internet browser/operating system/email program enabled?

☐ Yes	☐ No	☐ Don't know

Q5. Do you teach your child to use a child-friendly search engine on your home computer?

☐ Yes	☐ No	☐ Was not aware that there are child friendly search engines

Q6. Do you monitor the websites your child visits?

☐ Yes	☐ No

Q7. Do you talk to your child about using the internet safely?

☐ Yes	☐ No

If yes, what issues do you discuss?

☐ Strangers on the internet	☐ Spam, phishing	☐ Using search engines
☐ Downloading material safely	☐ Sharing personal information	☐ Using passwords
☐ Other (please specify)	☐ Other (please specify)	☐ Other (please specify)

Q8. Have you received or researched any information on child e-safety initiatives?

Received information	☐ Yes	☐ No
Researched information	☐ Yes	☐ No

Q9. Would you like more information on how to teach your child to surf the internet safely?

☐ Yes	☐ No

APPENDIX C

Questionnaire for Teachers

Date: _____

Q1. Do you use the internet in school with your class?

☐ Yes	☐ No

Q2. Do you encourage your pupils to use the internet at home for further study?

☐ Yes	☐ No

Q3. Is the internet access in your school filtered?

☐ Yes	☐ No

Q4. As a teacher have you received or researched any information on child e-safety initiatives?

Received information	☐ Yes	☐ No
Researched information	☐ Yes	☐ No

Q5. Do you teach your class specifically about internet safety?

☐ Yes	☐ No

If yes, please specify the content of what you teach

_____
_____
_____

APPENDIX D

ACTIVITY

Strong Passwords

In this activity, students will build on their existing knowledge of passwords and password security. Students will learn to use easy-to-remember, but hard-to-guess words, mixing upper case and lower case letters, substituting numbers and symbols for letters to make passwords more complex.

This lesson can be used as a take-home assignment, a bonus on a spelling test, or as a group activity.

Objective

Students will be able to provide at least one example of a strong password that includes numbers, symbols, and upper and lower case letters.

Set up

Each student will need a small piece of scrap paper, activity page, a marker, scissors, and an index card with a vocabulary word written on it.

Pre-Assessment

On the scrap paper, students will write down a word that they think would make a good password. (NOT using any of their current passwords). Students do not need to include their name; this assessment can be collected as soon as students finish.

Body

The teacher will instruct students to look at the word "blue" on the first line of their activity page under the "examples" section.

The teacher will ask "do you think this is a good password?," followed up with "why?/why not?"
The teacher is looking for students to say that the password is short, and/or it is easy to guess.

The teacher will ask "what can we do to make "blue" stronger?
The teacher is looking for students to say add to it/make it longer/harder to guess.

The teacher will ask students to cut their activity sheet on the dotted line, and then cut out each square to make cards. Using their number/symbol cards, is there a way that students can spell "blue" by replacing a few letters with numbers? They will write down their answer on the next line of the activity page. (b1u3)

STRONG PASSWORDS - ACTIVITY PAGE

Examples:

b l u e _____ s h o e _____

r a i n f o r e s t _____

Vocabulary word:

_____

_____

Bonus words:

_____

_____

_____

_____

✂ –

1	2	3	4	5
6	7	8	9	0
!	@	#	$	%
*	&	^	?	-

APPENDIX D

CYBER BULLYING

Cyber bullying occurs when the Internet or mobile phones are used to harm other people in a deliberate, repeated, and hostile manner. This includes threatening, intimidating, harassing, or causing embarrassment to the victim. It often occurs in social networks, blogs, through SMS, email or instant messaging. In Brunei, it is common for people to express their anger or frustration through social networking sites such as Facebook, Twitter and Instagram. If these online posts are directed at a specific person, it could lead to cyber bullying. Most cyber bullies are often motivated by anger, revenge or frustration. Many do it for their own entertainment or to get a reaction.

BEST PRACTICES

- Be careful what photos and personal information you post on the Internet. Keep in mind that anything you post might be seen by anyone in the world.
- If someone has posted something negative about another person, do not "Like" the post. When you "Like" it, you are supporting the bully's behaviour.
- Do not assume a picture of someone you met online is real. Often, what you see on the Internet or on social networking sites is not true.

IF YOU ARE BEING CYBER BULLIED

- Do not react to a bully. It might only motivate them more.
- Do not reply to any messages from a bully.
- If you are being cyber bullied by someone on a social network, you can "Block" or "Unfriend" them.
- If you are being cyber bullied by phone, you could change your phone number.
- Do not delete messages from a bully. They can serve as evidence when you lodge a report about the bullying.
- Report the bullying to your parents or even to the police.
- Many social networking sites allow users to report cyber bullying. For example, you can report bullying on Facebook's Help Center.

SOCIAL ENGINEERING

Social Engineering is a technique to deceive people to reveal sensitive information which they would usually not share. It typically involves trickery for the purpose of information gathering, fraud, or access to computer systems.

BEST PRACTICES

- Do not share your password or personal information (e.g. Identity Card, credit card number, bank account) with anyone.
- Keep your private information to yourself.
- Be aware that social engineers will say anything to convince people to give out personal information.
- Never provide sensitive information via email, phone message or phone call.

APPENDIX D

انٹرنیٹ – ایک متاثر کن اور مثبت مقام

انٹرنیٹ ایک قابل حیرت وسیلہ ہے جو بچوں اور نوجوانوں کو متعدد ٹھوس طریقوں سے ایک دوسرے سے جوڑنے، آپس میں بات چیت کرنے اور متعدد طریقوں سے تخلیقی صلاحیتوں کا اہل بناتا ہے۔ تاہم، انٹرنیٹ بعینہٖ بناتا رہتا ہے اور ٹیکنالوجی کے استعمال سے متعلق آپ کے بچوں کی دنیا کو ہمیں ضروریات کو پورا کرنے کے قابل ہونے کی وجہ سے ایک چیلنج ہو سکتا ہے۔ کبھی کبھی آپ کو ایسا لگ سکتا ہے کہ آپ کے بچوں کے پاس آپ سے بہتر تکنیکی مہارت ہے، تاہم آن لائن اپنی زندگی کے نظم و نسق کے لیے اب بھی بچوں اور نوجوانوں کو مشورہ اور حفاظت کی ضرورت ہے۔

ایسے مسائل جن سے آپ کا بچہ انٹرنیٹ پر سامنا کر سکتا ہے وہ ان کی عمروں اور آن لائن سرگرمیوں کے لحاظ سے مختلف ہوں گے۔ ہم نے ممکنہ آن لائن خطرات کو ان 4 درجوں میں تقسیم کیا ہے۔

طرز عمل:
بچوں کے لیے ضروری ہے کہ وہ اپنی آن لائن سرگرمی کے خود پر اور دیگر افراد پر ہونے والے اثرات سے اور انٹرنیٹ میں ان کے ذریعہ بنائی جانے والی ڈیجیٹل فٹ پرنٹ کے اثر سے واقف ہوں۔ آن لائن خود کو گمنام محسوس کرنا آسان ہے اور یہ اہم ہے کہ بچے اس بات سے واقف ہوں کہ ان کے ذریعہ پوسٹ کی جانے والی معلومات کون دیکھ سکتا ہے اور ممکنہ طور پر کون ان کا اشتراک کر سکتا ہے۔ انٹرنیٹ استعمال کرتے وقت نجی معلومات کو محفوظ رکھنا اور اسے اجنبیوں کو فراہم نہ کرنا اہم ہے۔ غیر مناسب گفتگو، پیغامات، تصاویر اور طرز عمل کی اطلاع دینے کی اہمیت کے بارے میں اپنے بچے سے بات کریں اور یہ بھی جانیں کہ یہ کیسے ہو سکتا ہے۔

مواد:
بچوں کے لیے بعض آن لائن مواد مناسب نہیں ہوتے ہیں اور نقصان دہ یا ضرر رساں ہو سکتے ہیں۔ سوشل میڈیا، ٹیٹ ورک، آن لائن گیم، بلاگ اور ویب سائٹس کے ذریعہ دیکھے جانے اور استعمال کیے جانے والے مواد کے لیے یہ ضروری ہے، بچوں کے لیے اہم ہے کہ وہ آن لائن مواد کی معتبریت پر غور کریں اور اس بات سے واقف رہیں کہ یہ صحیح نہیں بھی ہو سکتا ہے یا جانبداری کے ساتھ لکھا گیا ہو سکتا ہے۔ اس طریقے سے مواد کا استعمال شروع کرنے کے لیے بچوں کو آپ کی مدد کی ضرورت ہو سکتی ہے۔ مصنف کی اجازت کے بغیر کاپی رائٹ مواد کا استعمال یا ڈاؤن لوڈنگ کے قانونی عواقب ہو سکتے ہیں۔

رابطہ کریں:
بچوں کا اس بات سے واقف ہونا اہم ہے کہ آن لائن بنائے گئے نئے دوست وہ نہیں ہو سکتے ہیں جیسا کہ وہ دعویٰ کر رہے ہیں اور یہ کہ جب ایک بار کوئی دوست آن لائن اکاؤنٹ میں شامل ہو جاتا ہے تو آپ کی نجی معلومات اسے دستیاب ہو سکتی ہیں۔ دوستوں کی فہرست کا باقاعدگی سے جائزہ لینا اور مطلوبہ رابطے ختم کرنا ایک مفید قدم ہے۔ آن لائن رازداری سیٹنگز کے ذریعہ بھی آپ ان معلومات کو اپنے مطابق سیٹ کر سکتے ہیں جن کو ہر دوست دیکھ سکتا ہے۔ اگر آپ کو فکر ہے کہ آپ کا بچہ کسی دیگر فرد کے ہمراہ مناسب جنسی رابطہ میں ہے یا رہا ہے تو یہ ضروری ہے کہ آپ اس کی اطلاع Child Exploitation کے ذریعہ آن لائن حفاظتی مرکز کو دیں (www.ceop.police.uk)۔ اگر آپ کا بچہ سائبر جرائم کا شکار ہوا ہے تو اس کی رپورٹ آن لائن یا آف لائن کرنی چاہیے۔ اپنے بچے کو اس بات کی تاکید کریں کہ اگر کوئی اسے آن لائن ڈرا دھمکا رہا ہے، اس سے اس کو تکلیف کا احساس ہو یا اگر اس کے کسی دوست کو ڈرایا دھمکایا جا رہا ہے تو فوراً اس کی اطلاع کسی معتمد بڑے شخص کو دینے کی کیا اہمیت ہے۔

تجارت پسندی:
آن لائن نوجوان افراد کی رازداری اور لطف اندوزی کبھی کبھی اشتہاری اور مارکیٹنگ اسکیموں سے متاثر ہو سکتی ہے جس کا مطلب نادانستہ طور پر آن لائن پیسہ خرچ کرنا بھی ہو سکتا ہے، مثلاً اپنی کیشن کے اندر۔ اپنے بچوں کی حوصلہ افزائی کریں کہ وہ اپنی نجی معلومات کو رازداری میں رکھیں، یہ سمجھیں کہ پاپ اپ اور اسپام ای میل کیسے بلاک کریں، ان ٹھوس پر جہاں ممکن ہو آن لائن خریداری (In-app) کو کیسے بند کریں، اور آن لائن فارم بھرتے وقت ایک فیملی ای میل ایڈریس استعمال کریں۔

اپنے بچوں کے انٹرنیٹ کے استعمال سے متعلق ان سے کھل کر گفتگو کرنے کے حقیقی فائدے ہیں۔ کیا آپ کو معلوم نہیں ہے کہ کہاں سے شروع کریں؟ گفتگو شروع کرنے سے متعلق یہ مشورے مدد کر سکتے ہیں۔

1. اپنے بچوں سے پوچھیں کہ وہ کن سائٹوں کو دیکھنا پسند کرتے ہیں اور آن لائن کیا کرنا پسند کرتے ہیں۔
2. ان سے پوچھیں کہ وہ آن لائن کیسے محفوظ رہتے ہیں۔ ان کے پاس آپ کے لیے کونسے مشورے ہیں اور انہوں نے یہ کہاں سے سیکھا؟ دوسروں کو کونسی معلومات دینا اور کونسی معلومات نہ دینا بہتر ہے؟
3. ان سے پوچھیں کہ کیا انہیں معلوم ہے کہ مدد کے لیے کہاں رابطہ کرنا ہے۔ سیٹنگز سے متعلق مشورہ کہاں ملے گا، رازداری کی سیٹنگ کہاں ہوتی ہے اور جن سروسز کو وہ استعمال کرتے ہیں ان پر رپورٹ کیسے کرنی ہے اور بلاک کیسے کرنا ہے۔
4. کسی اور کی مدد کرنے کی انہیں ترغیب دیں۔ شاید وہ آپ کو کچھ چیزیں بہتر طریقہ سے آن لائن کرنے کا طریقہ بتا سکیں یا ان کا کوئی دوست ہو جو ان کی مدد اور تعاون سے فائدہ حاصل کرے۔
5. غور کریں کہ آپ دونوں انٹرنیٹ کس طرح استعمال کرتے ہیں۔ ایک ساتھ انٹرنیٹ استعمال کرنے کے لیے آپ اور کیا کر سکتے ہیں؟ کیا ایسی سرگرمیاں ہیں جن کا فیملی کے ساتھ لطف لے سکیں؟