CYBER SECURITY AWARENESS LEVEL IN TEENAGE GROUP OF NEPAL

A

THESIS

BY

MAHESH KUMAR ADHIKARI

FOR THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF EDUCATION

SUBMITTED

TO

DEPARTMENT OF MATHEMATICS & ICT EDUCATION

CENTRAL DEPARTMENT OF EDUCATION

UNIVERSITY CAMPUS

TRIBHUVAN UNIVERSITY

KIRTIPUR, KATHMANDU

NEPAL

2018

Letter of Certificate

This is certify that **Mr. Mahesh Kumar Adhikari** , a student of Academic Year 2071/72 with Campus Roll No: 416, Thesis No. 5, Exam Roll No: 28710466 and T.U. Regd. No.9-2-57-740-2010 has completed this thesis under my supervision and guidance during the period prescribed by the rules and regulations of Tribhuvan University, Kirtipur, Kathmandu, Nepal. This thesis entitled on "**Cyber Security Awareness Level in Teenage Group of Nepal**" has been prepared based on the results of his investigation conducted during the prescribed period under the Department of Mathematics and ICT Education, Central Department of Education, University Campus, Tribhuvan University, Kirtipur, Kathmandu, Nepal. I recommend and forward that his thesis be submitted for the evaluation as the partial requirements to awards the degree of Master of Education.

…….

Assoc. Prof. Laxmi Narayan Yadav

(Head)

Date: …….

Letter of Approval

This thesis entitled "**Cyber Security Awareness Level in Teenage Group of Nepal**" submitted by **Mr. Mahesh Kumar Adhikari** in partial fulfillment of the requirements for the Master's Degree in Education has been approved.

Viva-Voce Committee

Signature

Assoc. Prof. Laxmi Narayan Yadav ……..

(chairman)

Rom Kant Pandey ……..……

(External)

Bhoj Raj Joshi ……

(Supervisor)

Date: ……

Recommendation for Acceptance

This is to certify that **Mr. Mahesh Kumar Adhikari** has completed his M.Ed. thesis entitled "**Cyber Security Awareness Level in Teenage Group of Nepal**" under my supervision during the period prescribed the rules and regulations of Tribhuvan University, Kirtipur, Kathmandu, Nepal. I recommend and forward his thesis to the Department of Mathematics and ICT Education to organize final viva-voce.

……

Mr. Bhoj Raj Joshi

(Supervisor)

Date:……..

DECLARATION

This thesis contains no material which has been accepted for the award of other degree in any institutions. To the best of knowledge and belief this thesis contains no material previously published by any authors except due acknowledgement has been made.

……....

Mahesh Kumar Adhikari

Date:……

DEDICATION

This work is affectionately dedicated to my father **Surath Bahadur Adhikari**, mother **Belmati Adhikari,** brother **Laxman Adhikari,** sister **Himu Adhikari** and **Laxmi Adhikari** as well as my whole family members and relatives, who gave me a great span of their life for what I am here now.

Defense Date: November 26, 2018

ACKNOWLEDGEMENT

First of all, I would like to express my sincere gratitude to respected supervisor Mr. Bhoj Raj Joshi, Lecturer of Department of Computer Application, Patan Multiple Campus Patandhoka, Lalitpur and visiting faculty member Department of Mathematics and ICT Education, T.U. Kirtipur, Kathmandu, for his invaluable inputs, constructive suggestions, useful comments and continuous feedback, comprehensive guidance during the period of thesis writing and support to accomplish in this study. His vigorous efforts made me present this research work in this final form.

My sincere gratitude goes to **Assos. Prof. Laxmi Narayan Yadav,** Head, Department of Mathematics and ICT Education, T.U., Kirtipur, Kathmandu, for valuable suggestion and inspiration to carry out the research work successfully. I would like to express sincere appreciation Mr. Abtar Subedi, Mr. Krishna Prasad Adhikari, Mr. Dipak Mainali, Mrs. Sharala Luitel, Mr. Arjun Singh Saud and all the lecturers of Department of Mathematics and ICT Education T.U. Kirtipur, for their guidance, advice and motivation. I would like to thanks, the principal and teacher and students of different five schools of Surkhet district for their kind help. Without their participation and support my research work would not have been possible. My sincere thanks go to my dearest friends Khagendra KC, Prem Bahadur Shahi and Mahesh Singh Mahata for their support, encouragement and suggestion.

I especially express my thanks to my all family members and relatives for love, support and guidance. This thesis would be impossible without them.
Finally, I specially express my heartiest gratitude to my family member's and my friends for their kind cooperation.

…….

Mahesh Kumar Adhikari

ABSTRACT

This research entitled **"Cyber Security Awareness Level in Teenage Group of Nepal"**. The main objective of this study was to identify cyber security awareness level of teenager and to identify recent level of practice on cyber security by teenager. These objectives covered answer of these research questions: what is the cyber security awareness level of teenagers in Nepal? How is the Practice level of cyber security by teenagers in Nepal? What are the reasons that teenagers are more open to cyber-attacks than others? To fulfill these objectives this research adopted survey design method. This study was conducted in different five secondary level schools of Surkhet district among hundred students. These students were choosing from teen groups (13-19) and twenty students had chosen per schools and totally research conducted into hundred students. In this study here were number of structured questionnaire for collecting data. Generally, data from this research was analyzed using statistical tools. It followed percentile to analyze and interpret the gained data. Tools were pre – formulated questionnaire. The data were presented descriptively through tabulation method.

On the basis of collected data, the major conclusions drawn from the study are listed as follows: Most of the teenagers have used social sites and different web tools to be updated with new technology and for learning. Among all respondents about equally distributed as have to and have not to email address. The study has found that majority of teenagers used strong password. Most of the respondents did not change password regularly. Most of the teenagers used long password to protect

their devices and social site profiles. There was not good in awareness level in the sense of cyber security as well as in practice level of its.

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

ARPA	Advance Research Project Agency
ATM	Automatic Teller Machine
CSI	Cyber Security International
CSII	Cyber Security Institute International
CSIT	Computer Science and Information Technology
COP	Child Online Protection
DDoS	Distributed Denial of Service
ETA	Electronic Transaction Act
ETDSA	Electronic Transaction and Digital Signature Act
IP	Internet Protocol
IT	Information Technology
ITU	International Telecommunication Union
KMPCD	Kathmandu Metropolitan Police Crime Division
MOS	Merchantile Office System
NRN	Nepal Resident Nepali
NASA	National aeronautics and Space Administration
RONAST	Royal Nepal Academy of Science and Technology

CHAPTER I

INTRODUCTION

Background of the Study

A teenager, or teen, is a young person whose age falls within the ranges from 13-19. They are called teenagers because their age number ends with "teen". Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, the internet, cyber space and the worldwide web. Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. Cyber Security refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cyber Security strategies include identity management, risk management and incident management. “Cyber Security “means protecting information, equipment, devices, computer, computer resource, communication device and information stored there in from unauthorized access, use, disclosure, disruption, modification or destruction that can be used to protect the cyber.

Cyber Security is the foundation of digital business and innovation. Cyber Security encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. Biggest Cyber Security threats in 2017 are: Malware-as-a-Service, Evolution of Ransomware, Email Security Still A

Challenge, Spyware On The Rise Causing Security Challenges, Shadow IT, or the "Dark Cloud," DDOS Attacks Escalating, Privilege Becoming Important In The Cloud. Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describe the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation’s top intelligence officials cautioned that cyber-attacks and digital spying are the top threat to national security, eclipsing even terrorism.

Awareness stimulates and motivates those people to take security seriously, being trained to care about security, and to remind them of important security practices. For this reason, awareness techniques should be creative and frequently changed. The internet can be a great source of entertainment and knowledge for teens. It is also a way that kids can socialize with friends, even if they no longer live in the same city, state, or even country. Unfortunately, the internet also has many negative aspects that can be a cause for concern. These negative traits can cause problems that

emotionally hinder a child, stunt his or her ability to learn, and may even threaten his or her life. For this reason, parents not only want to keep their kids safe, but they want to ensure that their kids understand how to surf the net safely as well.

Statement of the Problem

Cyber Security refers to preventative methods used to protect information from being stolen, compromised or attacked. We have some cyber laws also which helps to be secure to and from any cyber-attacks in cyber space. Although, these law and policies are only limited into paper task instead the real field no one aware from such policies and cyber security related tasks in the context of Nepal. For example now days so many people involved into internet minimum 1/2 hour per day many of times unknowingly, they have to hijacked in to internet, spoofing their crucial personal information unwarily by intruders such as personal data theft by hackers. So many times we can see in many social sites has been posted very crucial personal information like as phone numbers, personal feelings and working in status. Although, in such critical activities highly motivated and practiced by teenage group in the context of whole world due to their curiosity in the internet.

Rationale of the Study

Teens use the Internet as much, and in similar ways, as adults. But they also often engage in risky behavior such as downloading illegal copies of movies and music. Popular social networking sites, like Facebook, Twitter can also expose teens to a variety of security risks. In the concern of cyber security, In Nepal so many awareness programs are conducted now days. After the developing of cyber law and different policies as well as many challenges comes into Nepalese society to aware and how to teach teenage about such policies. Reason has been transparent with us

because in the internet era, so many information we should maintain in electronic way and should be shared into many regions with the help of using internet. But in many cases in the internet different cyber abusing activities can we seen. Those types of abuses are controlling through the concept of cyber security. It is only one idea to decrease their cybercrime activities done by teenage in learning environment. Therefore in the context of Nepal computer subject holds the unit on the cyber ethic in school and college levels. This research help us what we should do practice and how to aware for maintaining security in cyberspace.

Research Objective

The objectives are as follows

a. To identify cyber security awareness level of teenager.
b. To identify recent level of practice on cyber security by teenager.

Research Questions

Research Questions are as follows;

a. What is the cyber security awareness level of teenagers in Nepal?
b. How is the practice level of cyber security by teenagers in Nepal?
c. What are the reasons that teenage are more open to cyber-attacks than others?

Significance of the Study

For starters, a proliferation of cyber-attacks is causing increasing damage to companies, governments and individuals. Take the WannaCry attacks that happened in May 2017 as a significant example: the ransomware inscribed itself on roughly 300,000 computers and other digital software in over 150 countries, later called the "largest such cyber assault of its kind." Putting it simply, organizations need to respond to this increased threat by adopting strict Cyber Security measures. Hence, in

these days Increasing threats which includes everything from damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post -attack disruption to businesses, forensic investigation, restoration and deleted hacked data and systems, to name a few. So that Cyber security awareness has significant role to prevent and avoiding such harassment with us.

Delimitation of the Study

In this research there are five different secondary level of government schools were selected from Surkhet district of Nepal, where totally one hundred students were participated and twenty teen-students(13-19 age group) selected from each schools. Due to the lack of proper time, sufficient balance and expenditure other schools and students can't be select in this study. Like as, among different study methods survey method is selected for this research.

Operational Definition of key Terms

Cyber Security :- "Cyber Security "means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction that can be used to protect the cyber.

Awareness: - Knowledge or perception of a situation or fact. Specially, Teenagers should know how to use different social sites (facebook, twitter , LinkedIn etc) and other sites as well. Similarly, they should know how to keep password safe from others.

Teenage: - Age group from 13 to 19 year. In this research, teens are students from secondary level school.

Practice: - Teenagers should be used strong passwords, should updated them, should use proper software and apps for good health of PC and smart phone as well as to keep safe their data and information. They should use antivirus and other firewall programs to stay secure. They should keep private privacy to their social sites profile.

CHAPTER II

REVIEW OF RELATED LITERATURE AND CONCEPTUAL FRAMEWORK

This chapter first reviews the current cyber security theoretical frameworks in academic literature and provides the argumentation for the choice of the theoretical framework for this thesis. After that, a theoretical framework was developed for this particular paper and its model was graphically presented.

Review of Related Theoretical Literature

Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (Margare, 2016). One of the most problematic elements of Cyber Security is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment. The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk (KunwarKhulduneShahid, 2015).

According to Forbes, the global Cyber Security market reached $75 billion for 2015 and is expected to hit $170 billion in 2020. A new study from Wombat Security and Aberdeen Group shows that boosting Cyber Security awareness and education can reduce infection risk up to 70 percent (SteveMorgan, 2015). The history of cyber security began with a research project. A man named Bob Thomas realized that it was possible for a computer program to move across a network, leaving a small trail

wherever it went. He named the program Creeper, and designed it to travel between Tenex terminals on the early ARPANET, printing the message “I’M THE CREEPER: CATCH ME IF YOU CAN".A man named Ray Tomlinson (yes, the same guy who invented email) saw this idea and liked it. He tinkered with the program and made it self-replicating—the first computer worm. Then he wrote another program—Reaper, the first antivirus software—which would chase Creeper and delete it (RobertBellamy,2017).

Policy and Provision of Cyber Security of Nepal

The Internet was first introduced in Nepal in 1993 in a venture of Royal Nepal Academy of Science and Technology (RONAST) and Merchantile Office Systems (MOS) (Shakya, November 6,2007). Now almost all big cities have Internet facilities with local ISP. Following types of cyber crimes have been committed in Nepal:

- ATM pin steal
- Cloning of ATM Card
- Hacking
- Financial fraud in Internet banking
- Phishing
- Social networking related crime

These all Cybercrimes are handled by Nepal Police against the FIR. It is necessary to have a regulatory body and strategy to set standards, prevent and handle cyber security related issues. In general, Cyber Security strategy should be able to ensure: Confidentiality, integrity and accessibility of electronic information and services provided in cyberspace, Safegurding of electronic

communication networks, information systems and critical infrastructure against incidents and cyber attacks, Protection of personal data and privacy etc.

Cyber Security in Nepal

sn	Measures	Profile
1	Legal measures	The Electronic Transactions Act, 2063 (2008)
2	Technical measures	NCERT (9th of April, 2015)
		No official cybersecurity framework • to implement internationally recognized standards, and • to provide certification and accrediation of natioanl agencies and public sector professionals
4	Organization measures	No officially recognized natioanl or sector-specific cybersecurity strategy
		No national governance roadmap
		The Kathmandu Metropolitan Police Crime Division (KMPCD) is responsible for cybersecurity
		No officially recognized national benchmarking to measure cybersecurity development.
5	Capacity building	No officially recognized R&D program for cybersecurity standards, best practices and guidelines
		No educational and professional training programs for raising awareness, higher education and certification
		No public sector professionals certified under internationally recognized certification programs
		No government and public sector agencies certified under internationally recognized standards
6	Cooperation	No framework to facilitate sharing of cybersecurity assets across borders
		No program for sharing cybersecurity assets within the public sector
		No officially recognized program for sharing cybersecurity assets within the public and private sector
		Nepal is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services

Table 1: Cyber Security in Nepal updated by ITU on 10th march 2015

Proper cyber law must govern all the cyber activities. Nepal cannot be isolated from emerging technology and the problems raised by the technology (Singh, 2001). The cyber law of Nepal is on the process of development. Recent Ordinance of E-Commerce is a milestone of cyber law in Nepal. The division of cyber law is really a tedious task. It comprises a variety of laws. (Nagpal, 2004) Cyber law encompasses laws relating to :

- Electronic and Digital Signatures
- Cyber Crime
- Intellectual Property (IP)

ELECTRONIC TRANSACTION AND DIGITAL SIGNATURE ACT

(GON, 2061) The Electronic Transaction and Digital Signature Act (ETDSA) – 2061 is a foremost of its kind in Nepal. Certification Authority which is further divided into 12 sections and 80 clauses. The act has covered many aspects of creation, production, storage and transmission of electronic information and also the act has covered many facets regarding electronic fund transfers. The act has defined many terms related to cyber activities and also made provisions related to the same. It has a number of positive provisions and also the strong provisions of punishment against cyber crimes.

The act has many strong provisions for the electronic transactions and digital signatures. It has defined the terms – Computer, Computer Database, Computer Network, Computer System, Subscriber, Key Pair, Private Key, Digital Signature, Access, Certification Practice Statement, Electronic Record, Electronic form, Public Key, Information, Information System, Software, Government Body, Social Organization etc. The definitions of these terms are precise and generalized definitions have been made. The act includes the provision concerning electronic documents. It also has the terms for and certification. of electronic document and legal validation of electronic document and digital signature .

The tasks of stealing, deleting and altering computer source codes; prohibited access to computers; affecting the computer and information systems; publishing the illegal materials, breaking the privacy etc has been described as the crimes related to computers. As per the nature of crime, wrongdoers involved in hacking, deleting information, stealing documents, digital signatures and software, pasting wrong information and improper and illegal materials would be brought under the judicial inquiry. As per the provisions of the law, the government is fully authorized to punish

cyber criminals - both an individual or institution. Stealing, deleting and altering of the source code of the computers will be punished with up to two years of imprisonment and a fine of up to Rs.200,000 or both - based on the severity of their crime . The same punishment has been quoted for the one who does the unauthorized access of the computer information systems. Likewise, people have to pay Rs. 100,000 or face five year's imprisonment or both for pasting wrong information in the websites.

Developing Cyber Security Framework in Nepal

(RamhariSubedi**,** 2016) First Cyber Security Awareness Campaign by CSI in Kathmandu on June 2, 2016, Cyber Security International Nepal (CSI) conducted its first awareness campaign at the premises of different Secondary School. The awareness campaign was attended by the students and teachers of Secondary School. It was a success with numbers of interested students and teachers who eagerly wanted to know more about the cyber security and to overcome cyber threats and challenges.

With a powerful presentation the evolution on cyber security and information technology effect on our life in positive as well as negatively. With globalization people have been facing so many problems of hacking and phishing, virus infections and cyber terrors which can disrupt the personal as well as professional working cycle. And he stressed the need to work more closely together as a shared mission to safeguard computer networks from cyber-attacks, which even with development in digital world the cyber-crimes has been growing continuously and none of the sector is safe from its threats. Nepali cyberspace is prone to attack and Nepalese people lack awareness about cyber threats, with lack of knowledge workers and infrastructure in

related field. With real-life examples, facts and figures like- yearly loss due to cyber-attacks, mental stress and even death of people because of hacker attacks and others.

Students and teachers found this awareness campaign to be very interesting and informative, adding that Cyber Security Awareness Campaign is helping to lead the way towards the development of safer use of internet. The awareness campaign was successfully concluded. Nepal Police Crime Investigation Bureau also took a short session with the students. He came up with more practical implications of misuse of the cyberspace citing its consequences a culprit can face. He also presented many real cases where people have got into trouble unknowingly. He informed that social media is the sector in which almost 90% of the cybercrime incidents take place in Nepal. Students have to be aware about sharing information in the social media and be careful about using the cyberspace.

ITU –NTA Workshop on National Cyber Security Awareness in Nepal

(Sameer Sharma, p. 2015) ITU is the specialized agency of the UN for telecommunications and ICTs. Theme for all year celebrations: "Telecommunications and ICTs: drivers of innovation". It was founded in 1865 and it has 193 member states, 567 sector members, 159 associates, 90 academia also Headquartered in Geneva, 4 Regional Offices and **7** Area Offices. ITU:Regional Office for Asia and the Pacific: 38 member states, 132 sector members and associates ,17 academia are resides here. Global 2014-Mobile cellular subscriptions are almost 7 billion. And Almost 3 billion people online Mobile broadband penetration: 84% developed countries ,21% developing countries.Fixed broadband penetration: 27.5 % developed countries , 6 % developing countries, almost 3 billion people online(individuals using the Internet).

Importance of Cyber Security

- From industrial age to information societies
- Statistics and reports show that cyber-threats are on the rise- The likely annual cost to the global economy from Cybercrime is estimated at more than $455 billion *(Source: McAfee Report on Economic Impact of Cybercrime, 2013).*
- Developing countries most at risk as they adopt broader use of ICTs-E.g. Africa leading in Mobile-broadband penetration: almost 20% in 2014 - up from less than 2% in 2010
- Need for building Cyber Security capacity

Coordinated Response

Need for a multi-level response to the Cyber Security challenges

Key Cyber Security Challenges

Cyber Security not seen yet as a cross-sector, multi-dimensional concern. Still seen as a technical/technology problem.

- Lack of adequate and interoperable national or regional legal frameworks
- Lack of secure software and ICT-based applications

- Lack of appropriate national and global organizational structures to deal with cyber incidents
- Lack of information security professionals and skills within governments; lack of basic awareness among users
- Lack of international cooperation between industry experts, law enforcements, regulators, academia & international organizations, etc. to address a global challenge

Global Cyber Security Agenda (GCA)

(ITU, 2007) In 2007, Global Cyber Security Agenda (GCA) was launched by ITU Secretary General. GCA is a framework for international cooperation in Cyber Security. Since its launch, GCA has attracted the support and recognition of leaders and Cyber Security experts around the world. GCA builds upon five pillars:

1. Legal Measures
2. Technical and Procedural Measures
3. Organizational Structure
4. Capacity Building

Global Cyber Security Index (GCI)

The Global Cyber Security Index (GCI) aims to measure the level of commitment of each nation in Cyber Security in above five main areas.

Top Performers in Asia-Pacific

Table No. 2

Country – Asia Pacific	Index	Regional Rank
Australia	0.7647	1
Malaysia	0.7647	1
New Zealand	0.7353	2
India	0.7059	3
Japan	0.7059	3
Republic of Korea	0.7059	3

ITU Child Online Protection (COP)

(ITU, 2007) ITU launched the Child Online Protection (COP) Initiative in 2008 within the framework of the Global Cyber Security Agenda (GCA), aimed at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere.

Key Objectives of COP

- Identify risks and vulnerabilities to children in cyberspace;
- Create awareness of the risks and issues through multiple channels;
- Develop practical tools to help governments, organizations and educators minimize risk; and
- Share knowledge and experience while facilitating international strategic partnership to define and implement concrete initiatives

Empirical Research

The Internet plays an increasingly larger role in the everyday lives of our children. As a learning and communication tool, it offers them a wide range of opportunities. It is an invaluable source of knowledge and encourages creativity and imagination. Research has shown that three quarters of European children are online availing themselves of these opportunities.

Unfortunately, use of the Internet has negative consequences: risks are encountered. These risks range from exposure to inappropriate content, undesirable contact from strangers, and even cyber bullying. Children may not have the necessary skills or knowledge to manage these online risks. So what can we do to protect them and ensure that they enjoy a safer, online experience? Eliminating online risk is an impossible task. Efforts in the past have focused on reducing children's exposure to

risk by controlling their access. Parental controls and monitoring, age verification solutions, walled-garden online environments and child-only social networking sites are some of the ways this can be achieved. However research has shown that children can circumvent these measures. It also limits their opportunities and leaves children whose parents are not tech-savvy still at risk. It is clear that a more effective solution is needed.

We can empower our children with the necessary knowledge and skills they need to stay safe online. We can raise their awareness of the risks they face and educate them about the safety and security issues they may encounter. An Information Security Awareness program designed specifically for children will achieve this goal. It will encourage children to adopt safe computing skills and will promote good security practice. It will aim to make children aware not only of the risks they face, but also of the countermeasures they can utilize to protect themselves. This paper considers the need for an Information Security Awareness program for children.

It identifies the categories of risk children face online, discusses the results of a survey investigating children's online activities and outlines the objectives of an awareness program for children. By implementing such a program, the author believes that we can allow our children to reap the full benefits of the Internet and enjoy a safer online experience (Clara Brady,2010).

Conceptual Framework

A conceptual framework is the representation of the understanding of the theories by the researcher and his/her own conceptualization of the relationship among different variables. It is the visual representation of the presumed relationship of the concept or variables that were involved in the study. Furthermore, many people

in Nepal who have internet access are not aware of the capabilities of the internet. It is mostly used by young population living in the urban areas for social media and video sharing. In Nepal the internet is mainly seen as just a medium of communication. In contrast to this, in developed country, it is used as an inevitable tool for our daily lives. People have less experience and awareness of the ways the internet can be used since it is so ubiquitous in our surroundings.

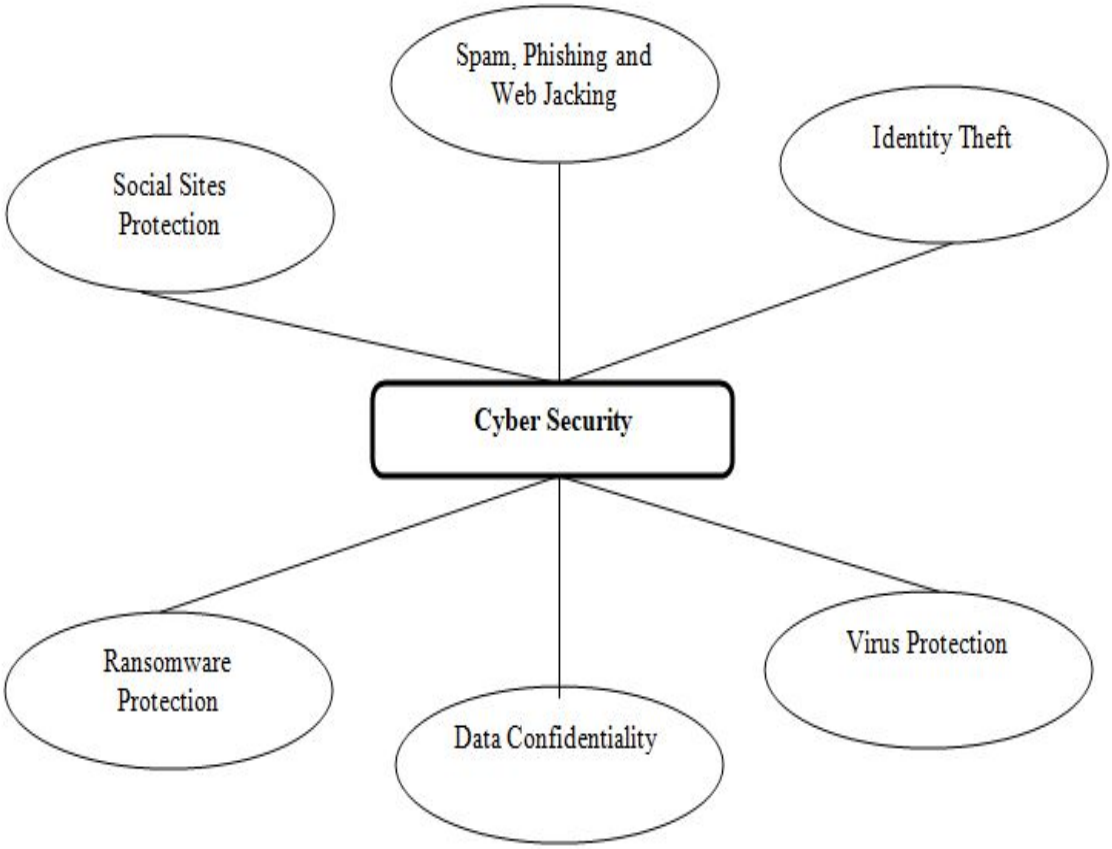

Figure 1 : Conceptual Framework of Cyber Security

Implications of the review for the Research

One of the most important parts of any research is reviewing the related literature. While reviewing the literature I have gone through various theoretical works and various empirical research studies. They all are related to some extent to my study area. After reviewing the research works, I got ideas on different existing theories related to my topic. Furthermore, from the empirical research studies, I have got information about the various procedures needed to conduct research study, regarding sampling strategy, use of tools, and analysis and interpretation procedures, I have gained valuable information from these research works. All these theoretical and empirical studies were very helpful to me during my whole research work. They became the milestone to make my task more information and reliable.

This research has so many information are containing regarding with Cyber Security awareness level and practice level, which should be very useful for research level, strategic level, application level or for delivery level to utilize the available resources to build nation, society , schools and home. First of all, It gives base idea to build suitable and sustainable national level cyber law and rule/regulations as well as for policy making, now which seems as very weak in the context of Nepal. Similarly, this research is useful for Teenage who are currently standing in focal point of cyber-attacks and cyber bulling. They have high level awareness about any cyber activity after the completion of this research due to this research totally focused on Teenage group. It was also very useful to teacher and their parents to monitoring what are they doing in internet and they can easily find out are they using internet in right way and their awareness level. It also gives way to further research based on this research in related area.

CHAPTER III

METHODS AND PROCEDURE

In this study, survey method adopted to fulfill the research objectives. To fulfill the objective of this study here are some number of structured questionnaire, which has utilized on some purposefully selected schools whereas meeting with related principle of those schools and to notify him to the purpose with the kind request for helping me. After that with the help of principle and other teachers 20 teen students are purposively selected for this survey in each five different schools of Surkhet district to fulfill my research objectives. The following methodology was adopted or used to conduct the research in order to fulfill the objectives of the study. Methodology and procedures are the vital elements of a research study. If any research work follows appropriate methodology and procedures, it obtained its objectives easily. Appropriate methodology helps the researchers to go in a right path in his/her research work. This chapter incorporates design of the study, population, sample and sampling strategy, research tools, sources of data, data collection procedures, ethical consideration.

Design of the study

Research is a kind of work or study which is done to find out truth or evidence on something. The research topic itself reveals the nature of the research to be undertaken. To be precise, the researcher adopted survey research design. To define the survey research, various scholars have put their views forward. According to Cohen et al. (1985, cited in Nunan, 1992, P. 140) survey are the most commonly used descriptive methods in educational research and may very large scale government

investigation to small studies carried out by a single researcher. Survey can be both descriptive and analytical surveys operate with hypothesized predictors or explanatory variables that are tested for their influence on dependent variables. To sum up survey is the descriptive research which deals with clearly defined problems and objectives. It is used for collecting data in most of the areas. The purpose of the survey is generally to find out the opinion, beliefs and attitudes on a certain issues as well as to find out behaviors of different professionals which are quite related to subjectivity of the study. Cohen et al. (2010, P. 208) present the following characteristics of survey research. It collects data on one – short basis and hence is economical and efficient. It represents wide target population. It generates numerical data. It gathers standardized information. It captures data from multiple choice, closed question, test scores or observation schedules.

To summarize, my study was based on survey research designs. I used survey design because my study is to find out the teenage/students awareness level on the Cyber Security. Survey research was done to derive the actual situation of the phenomena by observing it. So, I had used survey research design for my study.

Population and Sample

Population

There are many Government and many Private Schools in Surkhet district. The target population of my research was whole students in Surkhet district whereas students from teen group (13-19) as well as studying in secondary level. It made me easy to collect data from Surkhet district because my school life was spending there. So, I was already familiar with this place. I know more thing about their education system, schools, than other place.

Sample

A sample is a smaller, manageable version of a larger group. It is a subset containing the characteristics of a larger population. This research conducted in secondary level school of Surkhet district. Students studying in secondary level and from teen groups (13-19) for accomplish the research objectives. I had choose 20 students per school from these different five government schools of Surkhet district and totally it reached into 100 student because of time and expense constraints. It was not be possible to include all the population in my study. Therefore, I used simple random sampling procedure to select the sample from the population of the study.

Research Tools

The data was collected using survey method through the closed questionnaire. For doing that fifteen closed questionnaire were used. Questionnaire refers to a device for securing answers to a series of questions by using a form which the respondents fill in himself (W.J & P.K., 1952). In order to meet the research objective of the study, a set of questionnaire was used to meet the objectives. Answer of the research question was used to analyze the data. The questionnaire was developed on the basis of elements given in conceptual framework of the study and then questionnaire was administered to all sample students.

Pilot Study

To verify the achievement test, a pilot test was administrated. As a pilot test, the test was administrated among 23 students enrolled in secondary level school of Surkhet district. Twenty questions were used for pilot testing. Finally, the moderate fifteen questions were selected as the tools for this study.

Reliability of the Test

The reliability refers to the consistency of the result. Spearmen's split-half method and Karl Person's method were adopted to determine internal consistency by determining how each item on a test relates to all other items and to the total test. To confirm the test items were reliable the correlation was find out. For this, the questions were divided into two halves. In one half, the questions of even number were selected and in other side the question of odd number were taken. The correlation of these two halves was finding out by using Karl Pearson's formula and for finding the reliability of total test; the Spearman's formula was used. The correlation of these two halves was 0.86 and the reliability coefficient of total test was 0.92.

Validity of the Test

Validity is the degree to which a test measures what it is supposed to be measured. The achievement test paper was shared with the supervisor and subject expert for content validity and he suggested that the test items are acceptable. The opinion of all the subject expert was taken. The test items covered the fundamental knowledge for securing their identity, data and information with our current cyber policy. For expert validation, it was consulted with thesis supervisor and he suggested that the test items are good. From the pilot testing, it was seen that the questions are acceptable for this research study.

Item Analysis

In Item analysis, the difficulty level (p- value) and discrimination index (D-Value) of the test was computed to check which item accept for achievement test and also to check quality of the test item. Item difficulty index is a measure of the

proportion of examinees who answered the item correctly. The item discrimination index is a measure of how well an item is able to distinguish between examinees who are knowledgeable and those who are not, or between masters and non-masters. The researcher conducted the pilot test among 23 students of Shree Jivan Jyoti secondary school. After collected students response, first divide the total number of students into two groups which were appeared in pilot test by 50 % of high scorer and 50% of low scorer students from total. Out of them choose 27% high scorer students and 27% low scorer students. So, researcher took 7 upper 27% and 7 lower 27% scores students out of 23 students. By using statistical formula, only those item were selected whose P-value was ranging between 26% to 74% and D- value was ranging between 0.20 to 1.00. The other items were rejected and modified. The 5 item was rejected from 20 objective questions. After cancelling and modifying the items, the refined instrument of achievement test was prepared.

According to Kelly, T.L. (1939) the difficulty level and discriminating index values were calculated as follows:

Here the items were analyzed in terms of difficulty level and discriminating index.

Difficulty level (P)

It is the percentage of students able to pass each item. It takes value ranging from 0 to 100.

$p = \frac{R}{T}$ x 100%

Where,

R = Total no of students who gave correct response.

T = Total no of students.

Decision was taken by using following table.

Table No. 3

Difficulty level 'P'	Conclusion
Below 30%	Rejected (Very difficult)
30% to 70%	Accepted
50% to 60%	Good
Above	Rejected (Very easy)

Discrimination Index (D)

Discriminating index is a capacity which differentiates the strong and weak students.

The D value of each item was calculated by using following formula.

$$D = \frac{R_u - R_l}{\frac{T}{2}}$$

Where, R_u = No. of correct response from 27% of upper scoring students.

R_l = No. of correct response from 27% of lower scoring students.

T = No. of correct response from 27% of both upper and lower scoring students.

The decision was taken by using following table:

Table No.4

Scale	Conclusion
Above 0.35	Excellent
0.25 to 0.35	Good
0.15 to 0.25	Marginal
Below 0.15	Correctional

Source of data

I have used both primary as well as secondary sources of data for my study.

Primary sources: - Students.

Secondary sources: - Online posts, newspapers, portals, and different organizations reports.

Data Collection Procedure

When a researcher, follows appropriate data collection procedures he/she can easily gain the -required data. To collect the required data for this study, should be used the following procedures. At first, I prepared required separate set of questionnaire for students. Then, I built good rapport with students. Then, I had taken permission from concerned personnel or with the authority. Then, twenty students were selected from secondary level using purposive sampling strategy. Here, followed purposive sampling procedures to select my respondent. I was provided questionnaire to selected students. After the allocated time is over, I was collected the distributed questionnaire from the students. Finally, I had given thanks to them for their cooperation.

Data analysis procedures

After the collection of data, the researcher needs to organize the data to come to conclusion. The searcher decides to analysis the data as per his /her purpose nature of study and convenience. Generally, data from this research is analyzed using from quantitative research is analyses using statistical tools. This research followed statistical analysis such as percentile to analyze and interpret the gained data. I do so because my tools were pre – formulated questionnaire. The data gained from such tools can be analyzed by using mixed method.

Ethnical consideration

Ethnical consideration is one the most valuable ornament that a re-searcher should follow while conducting his/her research work. To accomplish research work was considered the following ethics: Researcher was conducted my survey by taking permission of authority. Researcher kept the response of the respondents' confidential one. All the ideas generated in this research are my own except from the cited ones. Researcher have tried to keep it safe from plagiarism.

CHAPTER IV

ANALYSIS AND INTERPRETATION OF RESULTS

In this chapter the researcher was discuss and present the analysis and interpretation of collected data from the sample. These data were presented descriptively and through tabulation. On the basis of collected data, the result was derived in term of awareness level of teenagers in Cyber Security. This chapter is mainly concerned with the analysis and interpretation of data which was collected from hundred teenager students from five different schools. Within them, all schools are from government schools. The data gathered from different sources were analyzed and interpreted under the two themes via cyber security awareness level of teenagers and level of practice on cyber security by teenagers.

A set of questionnaire consisting of closed ended questions was developed as a research tool. Teenager's general information from secondary level has been included in the first section. After that objective questions are included in second section. The closed-ended questions related to both cyber security awareness level and practice level of teenagers. Regarding statistical description, frequency and percentage was the main for the data analysis. if the responses were more than fifty percent, it was considered as high awareness level as well as if less than fifty percent deliberated as the low awareness of teenagers.

Analysis of Data and Interpretation of Results

The Collected data are analyzed, interpreted and discussed under the two main heading as per need of objectives of this study. These two main headings were as follows:

a) Cyber security awareness level of teenage

b) Cyber security practice level of teenage

This first heading further comprises different sub-headings, which are discussed in the following sub-sections.

Cyber Security Awareness Level of Teenage

The responses from the student of secondary level, regarding the awareness level of cyber security are analyzed and interpreted under the following sub-headings:

Social Sites

Table No. 5

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	Profile on social sites (Facebook,twitter)	94	6
2	They are Private	21	79

The above table shows that maximum respondents' i.e. (94 %) have their profile in different social sites. In another hands, only few profile on social sites are secure because almost all profiles i.e. (79 %) are not private. It concludes their data and any information in social sites are publicly available for all and it leads to vulnerable to attackers. So that, this table shows us there are lack of awareness level about cyber security.

E-mail Security/ spam protection

Table No. 6

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	Have an email account	53	47
2	Open spam e-mails	42	58

The above table shows that just more than average respondents' i.e. (53 %) have their e-mail accounts. In next statements, it shows us more than average(58 %) users are aware about we don't open our email from unknown peoples devices . So that, this table shows us their awareness level about e-mail is higher than average and it leads to us there is high awareness level about cyber security.

Data Confidentiality/Data and Information Protection

Table No. 7

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	Hacked by someone	7	93

In the concern of this above table, there are huge percentage i.e. (93%) of teenagers has not been hacked by anyone till now. It signifies to us there has been high awareness level about cyber security.

Table No. 8

S.N.	Statements	Response			
		Stealing Passwords	Loss Data and Information	Virus	Ransomware
		Percentage	Percentage	Percentage	Percentage
1	Hacking type	94	5	1	0

Where only seven percent of teenagers are hacked and among them larger group i.e. (94%) were suffered through the stealing passwords, only five percent teenagers suffered through the loss data and information and only one percent teenagers are suffered from virus and no one suffered from ransomware till now. It leads us there are high cyber security awareness level in teenagers.

Policy Related Awareness

Table No. 9

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	National strategy for COP	5	95
2	COP in academic curricula	14	86
3	knowing about cyber law of Nepal	44	56
4	Satisfaction in our government policy	22	78

Among the hundred respondents, the collected data reveal that majority of the teenagers i.e. 95% has said that here is no any national strategy for Child Online Protection (COP). Similarly, 86% teenagers responses in the side of here is not any proper COP courses in academic curricula. These both percentage shows us awareness level of teenagers about cyber security is very low. In another statement about awareness in cyber law of Nepal has also not good it has the percentage i.e. (44%) which is under the average but not so poor. Finally, in the statement of satisfaction in our government policy shows only 22% teenagers are satisfied. As a whole, it seems awareness level of cyber security of teenagers is not good.

Cyber Security Practice Level of Teenage

The responses from the student of secondary level, regarding the practice level of cyber security are analyzed and interpreted under the following sub-headings:

Identity Theft /Password Protection

Table No.10

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	Strong password	57	43

2	Password change	9	91
3	Password protected devices	88	12

Above table demonstrate us three things more than average number of teenager are using strong password today i.e. (57%). Similarly, almost all means (88%) teenager uses password to secure their devices. Which says us cyber security is high related to password protection. But in case of password changing, very poor result appeared with us i.e. only (9%) teenager updated their passwords in his/her daily life. It is relatively very poor practice about cyber security.

Table No.11

S.N.	Statements	Response			
		5 Character	8 Character	10 Character	15 Character
		Percentage	Percentage	Percentage	Percentage
1	Length of Password	4	22	37	37

Here , again above table is related to length of password, which shows how these passwords are easy to hack by hackers. Where there have been used lengthy passwords by most of the teenagers. Here, 37% teenagers have used 10 character length of passwords and equally 37% teenagers have used 15 character for length of passwords. It says us, almost teenagers have high practice level towards the use of password length.

Table No. 12

S.N.	Statements	Response			
		Per week	Per month	Rarely	Not Yet
		Percentage	Percentage	Percentage	Percentage
1	Update of Password	0	5	91	4

In the above table, mostly 91 % teenagers changed their passwords rarely but regularly when they feel should be need. Another side, least teenager's i.e. only (4%) teenagers has not been update password till now after opening their social accounts or e-mail and so on. Where, it can be concluded as there is high practice level of teenagers.

Virus Protection

Table No. 13

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	Auto run service Disability	12	88
2	uses of antivirus program	66	34

In the given table, many teenagers i.e. (88%) found in the category of who didn't disable auto run service in their devices. It is the main reason to make run able and spread all over the devices to virus. So we can say that, teenagers are not aware from auto run services. But in the case of second statement more than average means (66%) teenagers are found who used to the antivirus program in their daily life. It says that, they are aware in virus protection and it makes to secure the more than average marks of cyber security.

Ransomware Protection

Table No. 14

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	Backup data and information regularity	86	14
2	Disability of Unnecessary software	65	35
3	turn on firewall service in a computer	96	4

In the above table, here many i.e. (86%) teenagers are kept their data and information securely through the backup. Similarly, over average teenagers (65 %) disabled unnecessary software in their devices. Finally, almost all means (96%) teenagers found aware to turn about firewall services in a computer. It concludes that here is high cyber security awareness and practice level.

Overall Awareness and Practice level of Cyber Security

Table No. 15

S.N.	Statements	Response	
		Yes	No
		Percentage	Percentage
1	National strategy for COP	5	95
2	COP in academic curricula	14	86
3	Backup data and information regularity	86	14
4	Autorun service Disability	12	88
5	Disability of Unnecessary software	65	35
6	Have an email account	53	47
7	Profile on social sites(Facebook,twitter)	94	6
8	Strong Password	57	43
9	Changing password	9	91
10	Uses of antivirus program	66	34
11	Turn on firewall service in a computer	4	96
12	Participation on cyber security trainings	0	100
13	Hacked by someone	7	93
14	Devices are encrypted and password protected	88	12
15	Knowing about cyber law of Nepal	44	56
	Overall	43.2666667	56.7333333

While analyzing the responses to the whole statement, it was found that under the average i.e. (43 %) of the teenagers are aware besides this about 57% teenagers seems as unaware about cyber security. As a whole, they were not good aware regarding the practice and awareness level of cyber security but they are initiator of self-monitoring practices and it helps them to develop self-awareness.

CHAPTER V

SUMMARY, CONCLUSION AND RECOMMENDATIONS

This section includes the summary of the whole research study. The research study has been concluded in this section and its implication on policy level, practice level and further research has also been discussed. In fact, this chapter provides a brief summary of the whole study. As the concluding chapter of the study, it presents the major conclusion drawn from the discussion. It also provides some guidelines to implement the main findings in policy level, practice level and who wants to conduct further research under this area.

Summary

The value and importance of cyber security is undeniable. Cyber Security awareness is the worldwide issue for today's 21st centaury in the sense of our digital world. So, nobody can detach from its scope. The wide spread availability of the internet in different field (educational institutions, medical fields, military field and so on) makes cyber security dissemble almost everywhere and provides a more complexity about its awareness in our daily life. In these digital world we have so many online communities, social sites, different portals, websites , wikis and so on. Where instantly increased data, information and passwords breaches, email hacking, different social accounts hacking, web jacking, virus and ransomware attacking, cyber crimes and cyber bulling activities and most of the teenagers are unaware such criminal activities in the cyber space. So it is useful for the teenagers in teacher-student, student-student interaction, distance teaching and learning, to share learning materials with each other and to secure their profile and id in the cyber space.

The whole study is incorporated in five chapters. First chapters includes introduction, second chapter includes review of related literature and conceptual framework, third chapter includes methods and procedures of the study, fourth chapter includes analysis and interpretation of results and at last, fifth chapter includes summary, conclusions and implications. The chapter wise summary is presented as follows:

Chapter-one is about the introduction of the research. The title or topic of the research is "Cyber Security Awareness Level in Teenage Group of Nepal". It mainly deals with the background, statement of the problem, rationale of the study, objectives, research questions, significance and delimitation of the study. Under the general background it talks about the various purpose of cyber security awareness. This chapter mainly discusses about cyber security related with teenagers. An internet can be a great source of entertainment and knowledge for teenagers. Although, in such opportunities motivated and practiced by teenage group in the context of whole world due to their curiosity in the internet. They also often engage in risky behavior such as participated in anonymous criminals groups, downloading illegal copies of movies and music etc. Popular social networking sites, like Facebook, twitter can also expose teens to a variety of security risks. Hence, Cyber security awareness has significant role to prevent and avoiding such harassment with teenagers. The main purpose of this study was to find out the Cyber Security awareness level in teenage group. It was limited on hundred students aged between 13-19 from five different secondary level government schools of Surkhet district.

Second chapter deals with the review of related literature and conceptual framework of the study. All the related literature that found helpful for my study

which was reviewed and presented under the review of related literature. The theoretical review includes the concept about cyber security and its importance, cyber security framework in Nepal, condition of cyber law in Nepal , policy provision about cyber security and cyber security awareness program for teenagers. Implication of the review has also been discussed. Under that I have listed the points that would be helpful this study. And at last, this chapter presents the conceptual framework of the whole study.

Chapter three is al about the methodological part of the study which includes design of the study, population and sample, sampling procedure, data collection tools, data collection procedures and data analysis and interpretation procedures. In order to carry out the research under the title "Cyber Security Awareness Level in Teenage Group of Nepal" , the primary sources of data were 100 students and 20 students from each 5 different secondary schools of Surkhet district. All schools were purposively selected and all students were selected using the simple random methods. Data has been collected by using closed questionnaires. All together 15 questionnaires were made for analysis and interpretation. All questionnaires were designed for students to measure cyber security awareness and practice. After getting the approval for research study, data has been collected by following the previously mentioned process. With the permission from the authority, informants were contacted and provided some description about the research study. After that the questionnaires were distributed and they were collected later. This chapter also provides the whole procedures of data analysis and interpretation.

Fourth chapter is about the result and data interpretations. The results have been discussed in detail by analyzing students or teenager's responses. They were

analyzed by categorizing them into different items and their frequency and percentage were consulted by calculating teenager's responses. After that they were tabulated and brief descriptions of the tables were provided. The study was quantitative in nature. That's why data has been analyzed quantitatively analyzed. Questions in questionnaire were categorized into two items as related with awareness level and practice level of cyber security. The first heading further comprised of different sub headings. The collected data were analyzed and interpreted.

Finally, fifth chapter presents the summary, conclusions and implications of the study. The whole research study was summarized in this chapter. And some important conclusions were drawn from the study. Implications of the study have been presented by categorizing them into three levels. The implications that should be implemented at policy level are mentioned under policy level. The things that should be implemented at practice level i.e. in daily teaching learning activities are listed under practice level and the things that would be helpful for researchers to conduct further research under this area are listed in further research level.

Conclusion

All the teenagers' perception was found positive about the use of internet in teaching and learning process. All are active users of different web tools although they have lack of awareness in cyber security. There was not good in awareness level in the sense of cyber security as well as in practice level of its. In this section the major conclusions drawn from the study are listed as follows:

- Most of the teenagers have used Facebook, Twitter and other social sites to be updated with new technology.
- Some of the Facebook accounts were only in private.

- Among all respondents about equally distributed as have to and have not to email address.
- Often they did not use email address regularly and some of them open emails from unknown people's devices.
- The study has found that majority of teenagers used strong password.
- Most of the respondents did not change password regularly.
- Almost all respondents had used password protected devices.
- Most of the teenagers used long password to protect their devices and social site profiles.
- The study has found 91% of the students were rarely updated their passwords.
- Little bit respondents i.e. 12% did disable their auto run service.
- It was found that majority of the students used antivirus program in their devices.
- Only few of them were hacked till now and most of them suffered from stealing passwords.
- Almost all respondents has backed up their data and information regularly.
- This study found that maximum respondents disable their unnecessary software and turn on their firewall service.

By analyzing the data, it is concluded that cyber space becomes useful in teaching and learning for teenagers. It is mainly useful in teaching language aspects, literature, updating with current technology and affairs. Different social sites, portal, wikies help them for distance teaching, learning through chat and group discussion process. Whatever, they got such help from this cyber space actually they are in serious problem related to cyber security. They are very curious in cyber space but without proper awareness level and cyber security

related trainings. So, it is not much good condition in the concern of cyber security awareness and practice level.

Implications

This section includes the implications of this research study at different levels. They are:

Policy Level

This is highest level of implementation. The things that are implemented at this level would change the whole system of the country. Some of the implications of this study at policy level are:

- At present Cyber Security has great scope. It has minimized in to the teenagers. Hence, the policy makers should be aware with the scope and positive effects of cyber security in education system.
- Different types of awareness programs regarding the importance of cyber security to the learners are needed to be conducted.
- The policy makers should be aware about the increasing teenagers involved rate into the cyberspace for learning.
- The infrastructure must be managed throughout the nation for utilizing modern technology in education system.
- Academic curriculum must be designed by putting the sufficient cyber security awareness programs and current trends in technology for basic and secondary level students.
- The policy makers should develop sufficient cyber law for all and Child Online Protection (COP) strategy.

Practice Level

This is the level of actual implementation of the policies into classroom practice. Some of the implications of this study for this level are as below;

- The teacher should be trained to equip learners with the use of technology in the classroom.
- Internet facility and computer lab should be developed in the schools and colleges.
- The teacher should create separate group in social sites to deal with students in different study matter and for solving cyber security related problems.
- Teaching and learning process conducting through online and offline but with utilizing safe materials and places for downloading/ uploading learning materials.
- The teacher should encourage the student to use antivirus software and disable unnecessary software in their devices.

Further Research

Some of the implications that would be helpful for those who attempt to conduct research under this area are as follows;

- Further research in the field of cyber security must be carried in order to help the policy maker to determine the objective based on different learning groups.
- Further experimental investigation should be conducted by focusing on the cyber law in Nepal.
- There must be the investigation regarding the suitable technology and current trends in cyber space for embedding them into educational curriculum.

References

Acharya, C.P. (2013). *Use of ICT and web tools in English language Teaching* . An unpublished M.Ed thesis: T.U., Kathmandu.

Bardy,Clara.(2010,March 31). Security Awareness for Children. Retrieved from https://www.ma.rhul.ac.uk/static/techrep/2010/RHUL-MA-2010-05.pdf

Cohen, L. Manion, L. & Morrison, K. (2010). *Research Methods in education*. NewYork: Routledge.

Chaudhary,R.A.(2009). *Use of internet as language learning tool*. An unpublished M.Ed. thesis: T.U.,Kirtipur, Kathmandu.

GON. (2063). *The Electronic Transactions Act, 2063* . Kathmandu, Nepal.

GON. (2061). *The Electronic Transactions and Dital Signature Act*. Kathmandu, Nepal.

ITU. (2007). *ITU Global Cybersecurity Agenda (GCA).* Geneva: ITU.

Joshi,K.R.(2012).*Language used on Facebook.* An unpublished M.Ed. thesis: T.U.,Kirtipur, Kathmandu.

Khanal, D. (2017). *Research Methodology in Education*.Kirtipur, Kathmandu: Sunlight Publication.

Kunwar,Khuldune,Shahid.(2015,July 10).Cyber Security: Work in Progress Retrieved from http://www.technologyreview.pk/cyber-security-work-in-progress.pdf

MoE (2013). *Information and communication technology (ICT) in Education Master Plan 2013-17*. Kathmandu: MoE

Morgan,Steve.(2015,December 20).Cyber Security Market Reaches $75 Billion In 2015 Expected To Reach $170 Billion By 2020.pdf

Nagpal, R. (2004, December 7). *Introduction to Indian Cyber Law.* Retrieved from www.asianlaws.org: http://osou.ac.in/introduction-to-indian-cyber-law.pdf

RamhariSubedi, D. (2016, June 3). *Developing Cyber Security Framework for Nepal*, CSI International.

RobertBellamy.(2017, March 10). The History of Cyber Security — Everything You Ever Wanted to Know. Retrieved from https://sentinelone.com/cs.pdf

Rokaha,Surendra.(2014).*Facebook and Its Use in Language Teaching and Learning*. An unpublished M.Ed. thesis: T.U.,Kirtipur, Kathmandu.

Rouse,Margaret.(2016,November).Cyber Security. Retrieved from http://whatis.techtarget.com/definition/Cyber Security.pdf

Sameer Sharma, R. K. (15 september,2015). *ITU-NTA National Cybersecurity Awareness.* Kathmandu: ITU.

Shakya, D. (November 6,2007). *Country paper on ICT Country paper on ICT.* Kathmandu: National Information National Information Technology Center.

Singh, R. M. (2001). *Development of Science and Technology in Nepal.* Kathmandu: Royal Nepal Academy of Science and Technology.

Shrestha,Nita.(2016). *Awareness of EFL Teachers Towards Self Monitoring for their Professional Development*. An unpublished M.Ed. thesis: T.U.,Kirtipur, Kathmandu.

W.J, G., & P.K., H. (1952). *Methods in social research New York.* MacGraw Hill Book Company.

APPENDIX I

QUESTIONNAIRE FOR STUDENTS

This questionnaire is a research tool to collect data for my research entitled " **Cyber Security Awareness Level in Teenage Group of Nepal**" as a partial fulfillment of Masters of Education in MICT under the supervision of Mr. Bhoj Raj Joshi, Lecturer at Department of Mathmatics and ICT Educaton, Central Departement of Education, T.U. Kirtipur, Kathmandu. You are kindly requested to provide your valuable responses to the following questionnaire. The correct information provided by you will be of great value for completing my research. I sincerely assure that your responses will remain confidential and used only for the research purpose.

Name of School : Date:

Name of Student:

Class:

Age :

Roll no.

Attempt all the Questions.

Objective Questions

Q.No.1. Is there a national strategy for child online protection?

☐ Yes ☐No

Q.No.2. Are there any Child Online Protection education programs or academic curricula in Cyber security?

☐ Yes ☐ No

Q.No.3. Do you have a backup regularly taken to protect against threats such as virus?

☐ Yes ☐ No

Q.No.4. Has the Auto Run (or similar service) been disabled for all media types and network file shares?

☐ Yes ☐No

Q.No.5. Has the unnecessary software , including OS utilities, services and application has been removed or disabled?

☐ Yes ☐No

Q.No.6. Do you have an email account?

☐ Yes ☐ No

If yes, do you open spam emails?

☐ Yes ☐ No

Q.No.7. Do you have a profile on Facebook, twitter, LinkedIn or in other social sites?

☐ Yes ☐ No

If yes, Is your profile private? (Private means that only your friends can view your profile or limited in access to others)

☐ Yes ☐No ☐ I Don't know

Q.No.8. Do you use strong password to access on those account?(accounts may be gmail, facebook, twitter, youtube etc)

☐ Yes ☐ No

If yes, How long?

☐ Within 5 character ☐ Within 8 Character

☐ Within 10 character ☐ Within 15 character

☐ More..

What are they?

☐ Alphabet ☐ Numbers

☐ Special Characters ☐ Mixed Form

Q.No.9. Do you change your password?

Yes ☐ No

If yes, How often did you update your passwords?

☐ Per week ☐ Per month

☐ Rarely ☐ Not Yet

Q.No.10. Do you use antivirus programs in your device?(Devices means your desktop, laptop or may be Smartphone)

☐ Yes ☐ No ☐ Don't know

Q.No.11. Do you turn on firewall service in your computer?

☐ Yes ☐No ☐ I Don't know

Q.No.12. Have you participated in any cyber security related trainings?

☐ Yes ☐No

Q.No.13. Have you ever been hacked by someone?

☐ Yes ☐No

If yes, What type of hacking have you faced?

☐ Stealing passwords ☐Loss Data and Information

☐ Virus ☐Ransomeware ☐ More..

Q. No.14. Are mobile devices, tablet and your computer encrypted and password protected?

☐ Yes ☐No

Q.No. 15. Do you know and read about Cyber law in Nepal?

☐ Yes ☐No

If Yes , Are you satisfied in our government policy?

☐ Yes ☐ No

APPENDIX II

Verify the reliability of the test items by Split-half method

	X_0	X_e	x = X_0-A	y = X_e-A	x^2	y^2	xy
1	8	12	-10	-6	100	36	60
2	22	22	4	4	16	16	16
3	22	18	4	0	16	0	0
4	18	26	0	8	0	64	0
5	16	16	-2	-2	4	4	4
6	20	24	2	6	4	36	12
7	20	14	2	-4	4	16	-8
8	14	12	-4	-6	16	36	24
9	16	16	-2	-2	4	4	4
10	12	6	-6	-12	36	144	72
11	12	10	-6	-8	36	64	48
12	10	10	-8	-8	64	64	64
13	20	16	2	-2	4	4	-4
14	16	12	-2	-6	4	36	12
15	18	18	0	0	0	0	0
N=15	$\sum X_0$=244	$\sum X_e$=232	$\sum$x=-18	$\sum$y=-26	$\sum x^2$=332	$\sum y^2$=524	$\sum$xy=352

$$r_{oe} = \frac{\sum xy}{\sqrt{(\sum x^2 y^2)}}$$

$$= \frac{352}{\sqrt{(340.560)}}$$

$$= \frac{352}{\sqrt{(190400)}}$$

$$= 0.86$$

$$r_t = \frac{2r_{oe}}{(1+r_{oe})}$$

$$= \frac{2\ X\ 0.86}{(1+0.86)}$$

$$= \frac{1.72}{(1.86)}$$

$$= 0.92$$

APPENDIX III
LIST OF SCHOOLS

S.N.	Name of Schools	Number of Students
1	Shree Aadarsh Secondary School Surkhet	20
2	Shree Jivan Jyoti Secondary School Surkhet	20
3	Shree saraswati Secondary School Surkhet	20
4	Shree Shikhar Secondary School Surkhet	20
5	Shree Jana Priya Secondary School Surkhet	20

APPENDIX IV
LIST OF TOTAL RESPONDENTS

School: Shree Jana Priya Secondary School Birendranagar,Surkhet

S. No.	Name of Students	Class	Age
1	Radheka Sapkota	10	15
2	Anuradha Subedi	10	14
3	Smriti Dhakal	10	15
4	Smita Regmi	9	15
5	Binam Kandel	10	15
6	Mamata Subedi	9	13
7	Dinesh Ban Sanyasi	10	14
8	Sangam Gharti	9	14
9	Karishma Bohara	10	15
10	Dipendra Gautam	10	15
11	Yogendra Rana	10	15
12	Yogesh Sharma	10	15
13	Sudeep Kandel	9	14
14	Abhisek Rawal	10	17
15	Aakriti Rana Chettri	9	14
16	Tribhuwan Adhikari	10	16
17	Pawan Acharya	10	16
18	Nisan Khatri	10	16
19	Dipendra Nepali	9	15
20	Netra Bahadur Oli	9	16

School : Shree Saraswati Secondary Lekbesi -6,Surkhet

S. No.	Name of Students	Class	Age
1	Rita Khatri	11	17
2	Shanti kumari Thapa	11	16
3	Pradip Bajgai	11	17
4	Dhan Bahadur Khadka	11	19
5	Himal Rokaya	11	16
6	Dilmaya khadka	11	17
7	Durga Oli	11	17
8	Dil kumari Budha	11	18
9	Himal Gharti	11	16
10	Dil maya Hunching	11	18

11	Bima Gharti	11	18
12	Tika Kumari Magar	11	16
13	Aruna Gyawali	11	17
14	Janaki Gharti	11	16
15	Sunita Gaha	11	17
16	Lilawoti Budha	11	17
17	Dipa Kumari Khadka	11	17
18	Amrit B.K.	11	16
19	Purna Bahadur Gurung	11	17
20	Durga Gharti	11	17

School : Shree Shikhar Secondary School Bheriganga,Surkhet

S. No.	Name of Students	Class	Age
1	Ashish Thapa	10	17
2	Pabisara Oli	10	16
3	Laxmi Acharya	10	15
4	Purnima Bhandari	10	15
5	Dipa BC	10	16
6	Ganesh Dhaulakoti	10	14
7	Dhan Bahadur Khadka	10	16
8	Dhirendra Hamal	10	16
9	Radha GC	10	16
10	Puspa Singh	10	17
11	Parvati Basnet	10	15
12	Purnima Hamal	10	16
13	Tej Khatri	10	17
14	Suman Shaha	10	14
15	Hira Khatri	10	14
16	Bindu BK	10	16
17	Suresh Pokhrel	10	15
18	Keshab Pokhrel	10	14
19	Arjun Thapa	10	15
20	Mohan Khatri	10	15

School : Shree Aadarsh Secondary School Lekbesi -1,Surkhet

S. No.	Name of Students	Class	Age
1	Sunita Sunar	11	18
2	Lila Budha	11	17
3	Sita Budha	11	16
4	Bhadra Kathayat	11	17
5	Radha Paudel	11	19
6	Prtiva Sunar	11	15
7	Puja Aagri	11	15
8	Pavitra Paudel	11	15
9	Punam Paudel	11	17
10	Anu Nepali	11	17
11	suman Barali	11	17
12	Puspa Sijali	11	17
13	Jasodha Thada	11	16
14	Jharana Budha	11	16
15	Dhirendra Thada	11	15
16	Jhag Bahadur Phauja	11	16
17	Milan Sharma	11	18
18	Kamal Thapa	11	17
19	Dil Thada	11	16
20	Lelina Thada	11	16

School : Shree Jivan Jyoti Secondary School Lekbesi-4,Surkhet

S. No.	Name of Students	Class	Age
1	Nabin Kumar Adhikari	12	17
2	Tikaram Basnet	12	17
3	Dharmaraj Salami	12	17
4	Khagendra Gyawoli	12	19
5	Dilip Thapa	12	14
6	Tabita Oli	12	17
7	Reshma Basnet	12	18
8	Sapana Sinja	12	18
9	Sangita Oli	12	17
10	Dipika Khatri	12	19
11	Kamal Pun	12	17
12	Parvati Tiwari	12	19
13	Bhavana Sunar	12	18
14	Chanumaya Khatri	12	18

15	Prayanka Magar	12	18
16	Pramila Pun	12	18
17	Narayan singh	12	18
18	Nabin Adhikari	12	17
19	Prem Adhikari	12	16
20	Mahendra Oli	12	17