Securing Our Digital Natives: a Study of Commonly Experience Internet Safety Issues and a One-Stop Solution

Chandni Agarwal
Senior IT-Faculty
Maharaja Agrasen Model School
New Delhi, India
+91-8130808722
chandni1972@gmail.com

Akshath Singhal
Bachelors of Technology Student
Delhi Technological University
New Delhi, India
+91-9899016540
singhal.akshath97@gmail.com

ABSTRACT

With the exponential development of electronics industry, smartphones have become a common commodity found with almost everyone irrespective of the age group providing easy access to Internet. While Internet proves to be one of the best sources for learning almost everything, an unguided exposure to it may pose serious security issues and even lead to hampering of children's growth. In our study we found that the Internet Security related problems have been on an all-time high in the past decade. It is also found that the most affected age group was 13-20 years of age and that in most cases the issues could have been avoided or at least easily resolved if the family members of the cyber victims had been more aware. In India, cybercrime and victimization in the cyber space has remained a subject of great consternation, but lacks cognizance. This paper primarily focuses on digital awareness trends amongst people of various age groups and an initiative to help make society a safer place for everyone by providing a one-stop solution to the most commonly experienced Internet Safety issues in the form of free android app "Cyber Security Guide". This paper also highlights the key features and benefits of app. Our paper will also encompass the following: (a)Objectives (b) Introduction (c)Need for Internet Safety and Digital Citizenship (d)Case Studies (e)Research on Students' Problems (f)Development of CSAO (g)Probable solution to the problem (h)Salient Features of App (i)Response from our Users (j)Limitations (k)Conclusions and (l)Future Scope.

CCS Concepts

• Applied computing~E-government

Keywords

Malware; Virus; Cyber Security; Cyber Bullying; Defamation; Pornography; Spyware; Ransomware

1. INTRODUCTION

The mode of communication has changed drastically in the past few decades due to an important invention which took place somewhere around 1960s enabling computers to send and receive data leading to formation of what we now know as Internet. With development of new networking protocols and advancement of digital computers, all the information slowly made its way to the world-wide web. But this also led to a safety issue as all the information now became widely accessible. With introduction of technologies like e-commerce, social networking and e-banking in the late 20th century, the issue of Internet Safety became much more important and cyber laws were made stricter. However, the awareness about cyber threats and cyber laws didn't spread as fast as the access to Internet did. While various protocols were(and are being) developed to maintain safety of internet users and to block hackers, it could easily be observed that most of the cyber victims usually fall prey to cybercrime due to the lack of knowledge about cyber laws and safety issues. Proper awareness needs to be spread amongst people of our nation in order to make Internet use safer for everyone and contributing to development of a healthy environment for growth of the society. With the growing popularity of Bring Your Own Device(BYOD) concept and 1:1 learning initiatives in schools and colleges, emphasis needs to be on digital citizenship and on awareness spreading campaigns. The presence of a cyber-safe environment becomes all the more important due to the Digital India programme launched by the Government of India as a step towards e-governance. It needs to be ensured that minors access Internet under adult supervision and that these adults have proper awareness and knowledge to avoid exposure of children to inappropriate material and save them from becoming victims of cyber-crime.

Digital Citizenship is an umbrella term for the society that refers to the norms of appropriate and responsible use of technology i.e. it defines the considerate use of technology. It is a helpful concept for teachers and parents to understand what technology users, students and children should know to use technology appropriately. The need to setup a Cyber Culture full of awareness is need of the era.

The remainder of the paper is organised as follows. Section 2 provides an overview of the major safety issues and threats which users have to deal with and the need for Internet Safety. Section 3 deals with the case studies conducted at institutional level followed by analysis of surveys conducted in Section4. Section 5 focuses on development of CSAO. This is an initiative to contribute towards a cyber-safer world, followed by the probable solution to all the problems in Section 6 and the salient features of this mobile application solution in Section7. Section 8 gives a glimpse of the benefits that this app may provide to the society, followed by case studies of responses from our users in Section9. The limitations are discussed in in the 10thSection and concluding remarks form the 11th Section with some idea on Future scope in Section 12.

2. NEED FOR INTERNET SAFETY

Internet Safety is a very broad term and there is still no clear concept regarding the protection of Digital Natives in cyberspace. The term Internet Safety refers to the steps or precautions that should be taken while using Internet in order to ensure safety of

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICEGOV '17, March 07-09, 2017, New Delhi , AA, India
© 2017 ACM. ISBN 978-1-4503-4825-6/17/03...$15.00
DOI: http://dx.doi.org/10.1145/3047273.3047303

personal information and to avoid cyber threats. Cyber threats may be defined as a malicious attempt to damage or gain unauthorized access to a computer network in order to perform a Cyber-crime. With the boom of globalization and Social Networking sites, people have become more vulnerable to cyber threats like cyber bullying, stalking and cyber defamation. Easy access to Internet has also exposed people to threats like: Spyware, Ransomware, Phishing, Distributed Denial-of-service attack and Hacking. But for the kids and teenagers, one of the biggest problems that occurs is the exposure to material considered as inappropriate for their age group otherwise. A few years ago, teenagers would have to go and request a shop owner or librarian to provide them with pornographic or adult material or magazines. In such a case, it was easy to identify their age and refuse access to such material. But now-a-days everything is accessible to them at the click of a button. As the number of Internet users increases rapidly, internet safety has become a matter of great concern for everybody. It can easily be inferred from the given data in “Table 1: Internet users by country” that internet is no longer a luxury; instead it has become a commodity of daily use. [4] It has incorporated itself so much into our life that it is impossible to think about excluding it from our existence. We see our teenagers sitting with their smart gadgets all the time frenetically typing messages into their cell phone. Our smart whiz-kids can beat us in gaming or types faster than us. All of them are “Digital Natives, born in the online age. They all have access to networked digital technologies and the skills to use those technologies.

Parents and teachers are on the front lines. They have the biggest responsibility and the most important role to play. It’s often the first thing that people mention on their list of concerns about what their kids are up to online. Digital Native’s time online is spent without adult supervision; he is far less likely to have an adult nearby to help him process the disturbing material he has just encountered. Let’s start with the most common example that worried parents raise: pornography. In the online context, parents often point first to the concern that a child might be more likely to be exposed to all forms of pornography than they would in an offline setting. It’s true: Porn is far easier to come by online than it was before the Internet’s existence.

A single Google search using a remotely naughty word turns up many varieties of pornography, just a click or two away and free for the viewing. There are literally hundreds of thousands of adult sites on the Internet, which doesn’t take into account the large number of amateur videos posted to general-purpose video sites fact. According to one set of surveys, 42 percent of kids between the ages of ten and seventeen have seen porn online. Two-thirds of the time the exposure was unwanted, mostly the result of the use of file-sharing programs; but in at least one-third of the cases, the children sought out the material.

The second difference is that the material is easy to access, regardless of age. In the pre-Internet era, a young person might have to convince a store clerk that he was of a certain age before the clerk would turn over a pornographic magazine from the top shelf in exchange for cash. These intermediaries were hardly fool proof, from a parent’s perspective, but at least they might function as speed bumps. The kid had to come up with cash and a gullible salesclerk, at a minimum—or perhaps a salesclerk willing to accept a small bribe. A greater barrier still, the child would also have to confront the high potential for shame: shame at being caught buying the magazine, shame that the clerk happened to be in his sister’s class in high school, or any number of other scenarios that are less likely to attach in the context of accessing images on a laptop in a bedroom at home behind a closed door.

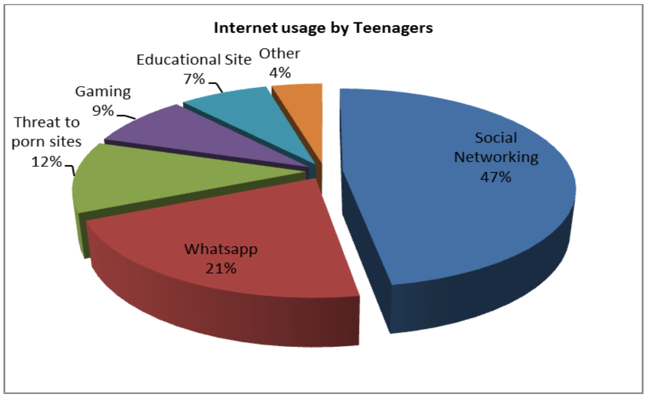


Figure 1. Internet Usage by Teenagers

Table 1. Internet Users by Country (2016)

#	Country	Internet Users (2016)	Penetration (% of Population)	Population (2016)	Non-Users	Users 1 year change(%)	Internet Users 1 year
1	China	721,434,547	52.2 %	1,382,323,332	660,888,785	2.2 %	15,520,515
2	India	462,124,989	34.8 %	1,326,801,576	864,676,587	30.5 %	108,010,242
3	U.S.	286,942,362	88.5 %	324,118,787	37,176,425	1.1 %	3,229,955
4	Brazil	139,111,185	66.4 %	209,567,920	70,456,735	5.1 %	6,753,879
5	Japan	115,111,595	91.1 %	126,323,715	11,212,120	0.1 %	117,385

Cyber bullying is the intentional use of any digital medium, including text-messaging, pagers, and phone calls, to harm others. And cyber bullies are, in most respects, like their classic schoolyard counterparts. Delhi has been described as the capital city, but eventually it is turning to stalkers paradise. A paradise, where two women in Delhi were recently stabbed to death by the stalkers. According to latest data, from National Crime Records Bureau, a major chunk of people arrested for stalking fall in the age of 18-30 age group. Rejection, separation, insult and resentment are the causes which contribute to stalking. And not only Delhi, but the whole country suffers from these issues. Though, cases of stalking in the country are on the rise, (shockingly) it is still considered as minor offence. Stalking has become a rampant phenomenon and it needs to be curb.

We have also talked how inextricable it has become keeping in view the fact that India ranks second in the list of countries with maximum people online, partly because of the surge of social media and partly because of other concerns including the vast reserves of information which can be accessed at the click of a button. The most fascinating fact here is that the change in Internet Users in India is much higher than in any other country. With an increase of more than 100 million Internet Users per year, India will soon have the largest Internet Users Base in next few years. This leads to the need to have an efficient system for security and privacy concerns of the billions of internet users all around the world. Among the content that the internet provides to all in an indiscriminately manner lies the problem of the need to look for ways to enhance security of its users. With the recent rise in cases of cyber bullying and harassment it has become even more imperative to have rules and implement them too and rather strictly at that. It is also found that the teenagers spend most of their online time at social networking sites making them vulnerable to all sorts of cyber threats, be it Cyberbullying, cyber defamation, stalking, and exposure of content which may be inappropriate for their age-group (pornography and violence). But these are not the only ones that fall prey to Cyber threats. Threats like frauds, cyber defamation and bullying may occur with anyone. Cases of hacking, stealing of personal information and ransomwares have increased recently causing loss of billions of dollars per year to the world economy. The annual estimated cost to the global economy by Cyber Crime is estimated to be $445 billion.

Not only is cyber safety causing loss to economy but also hampering the growth of children and society as a whole. Hence, there is a strong need to deal with these issues strictly and develop a Cyber Safe environment for all.

Researchers at Harvard have been working towards a deeper understanding of the very concept of digital safety for citizens of developing countries like ours [13] and to use cyber networking and digital systems as an important learning tool. [5]

3. METHODOLOGY AND DATA SELECTION

Keeping the increasing number of cases of Cyber Crime and Cyber Victims in the schools in mind, and the fact that the problems faced by the people needed in depth analysis, various case studies were conducted at school and locality level in order to understand the problems better. The methodology used was practical qualitative approach. Various cases reported to different school counsellors and to our experts were first sorted on the basis of the intensity of problem and its impact on individuals. The victims were then contacted and one-to-one sessions conducted for in-depth analysis of the problem. Some of these cases have been mentioned in the following pages after taking permissions from the victims.

3.1 Case Study 1

It was found that a fight was planned against a student by his classmates on internet using social networking site. The fight could not be avoided but the students responsible for planning this fight were caught later and the chat history was used as a proof of the crime when handed over to the police. The incident took place because of acts of cyber-bullying that had been going on from past couple of weeks and use of abusive words on the Facebook wall. Students were not aware and didn’t report the cases of bullying earlier which might have helped avoid this conflict. The case took a violent form and police had to be involved.

3.2 Case Study 2

The bullying form has been changed from the physical classroom walls to the virtual world with no boundaries. Students were found bullying and teasing their classmates. The matter remained unreported and hence unresolved. It was only when the things went violent that the authorities resolved it. It was because of the hesitation and peer pressure that the victims felt shy in reporting the issue to the authorities.

3.3 Case Study 3

Objectionable photos of a teenage girl were clicked and leaked on a social networking site by some people. Due to lack of awareness the photo got spread over the internet leading to worsening of the situation. The issue was finally resolved when the authorities were contacted to remove the images along with the government authorized identity card of the victim.

Table 2. Awareness Survey Conducted by CCVC

Awareness of cyber security among Indian internet users	**Yes**	**No**
1. Knowledge of minimum age to join cyber communities like Facebook, Orkut, Myspace etc.	56.2%	43.8%
2.Allow others to use one’s own email id / profile id /passwords etc.	46.6%	53.4%
3. Use safety tips like filtering emails, locking personal albums and information, personal walls of social networking sites etc.	69.9%	30.1%
4. Mail back to unknown senders of spam / pornographic / erotic /phishing mails	37.0%	63.0%
5. Share personal information / emotions with virtual friends / chat room partners etc. whom you don’t know in real life	74.0%	26.0%
6. Believe in controlling free speech while communicating in the cyber space.	37.0%	63.0%
7.Read policy guidelines of social networking sites, ISPs etc.	28.8%	71.1%
8. Use pseudo names	45.2%	54.8%

The above table depicts the baseline survey statistics conducted by CCVC (Centre for Cyber Victim Counselling) on the Indian users.[2]

It is evident from the above table that among a total of 73 respondents, 56.2% are aware of the basic age limit for joining any cyber community/groups/social networking sites. It is to be noted that these 73 respondents are adults and majority of them are ‘Internetting’ for more than 5 years. This particular assessment was necessary as many of these respondents have children who are either in pre-teens or teenagers or even young adults. Most of the respondents felt that the cyber communities or social networking sites or chat rooms etc. should be only used by matured users. These respondents are also aware that impersonating as a child (when the user is an adult or a young adult and camouflages as a pre-teen or teenager to groom women and children for cyber nuisances including sexual crimes) in the chat rooms or social networking sites and trapping other children or women especially, are ethically wrong and this can lead to severe legal problems as well.

4. PROBLEM ANALYSIS

Due to the pressing need for awareness regarding internet safety issues, we decided to conduct a survey in order to assess the awareness level of students and their parents. Two surveys were conducted for students and their parents to get a glimpse of the issues they had to deal with. The surveys were carefully designed in order to cover major issues. Various previously held surveys were first examined along with the results they produces to optimize the question selection process. The results of the survey proved to be the basis for the development of Cyber Safety Awareness Organization Guide.

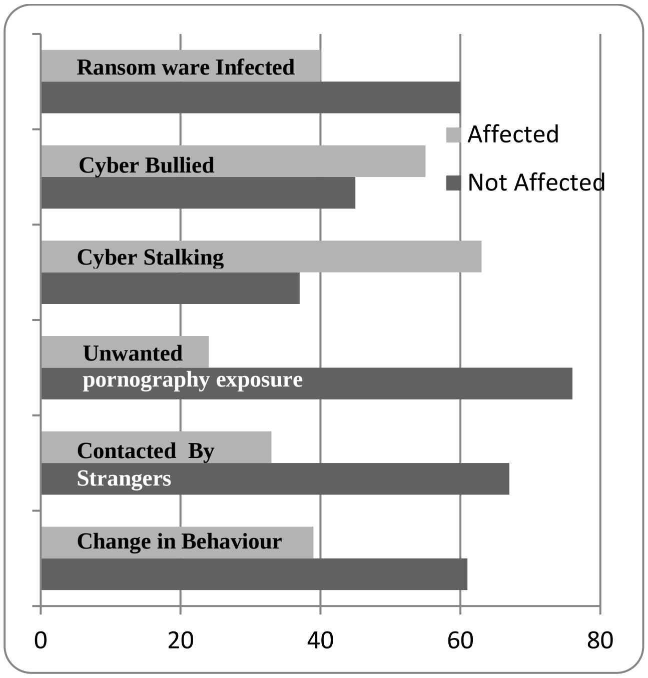


Figure 2. Results of Survey conducted on Students

One-to-one talk sessions were conducted with student representatives from different classes to discuss the commonly faced problems under the supervision of a professional counsellor. The findings and results of the above mentioned practices helped in arriving at the following result. The most common issues are:

- Students were hesitant to talk about cyber safety issues.
- Lack of awareness amongst parents led to a communication gap in terms of the cyber world.
- Lack of professional Cyber Experts.
- Peer pressure proves to be a hindrance to students and hence they aren’t able to share their problems about cyber-crimes.
- Information about Internet security is widely scattered and no one-stop solution is available.

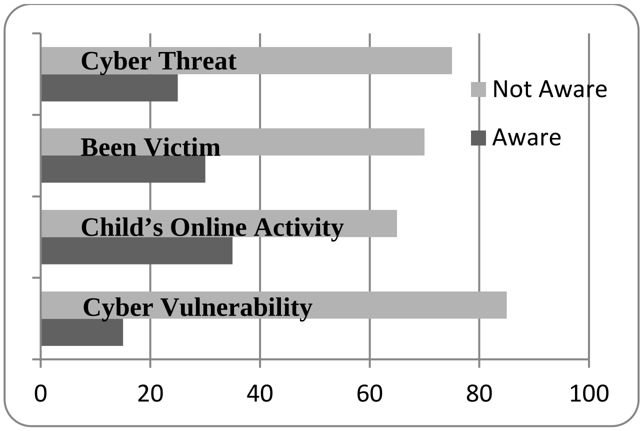


Figure 3. Results of Survey conducted on Parents

Table 2. Awareness Survey organized while research

Knowledge of being Victimized	**Yes**	**No**	**No awareness**
Had bad experience in the social networking sites	61.6%	38.4%	
Received abusive / dirty mails in inboxes from known / unknown sources	78.1%	21.9%	
Has experienced hacking (either directly / indirectly)	78.6%	19.4%	2%
Has experienced cyber stalking	37%	50%	13%
Has experienced phishing attacks	50%	42%	8%
Has been impersonated by email account / social networking profiles /websites etc.	38.3%	50.4%	11.3%
Has seen his/her ‘cloned’ profile/email ids	78.2%	10.2%	11.6%
Has been a victim of defamatory statements in the cyber space	68.8%	13.8%	17.4%
Has received hate messages in their inboxes/message boards	76%	16%	8%
Has seen his/her morphed pictures	66%	24%	10%
Has been bullied	80%	12%	8%
Has experienced flaming words from others	70%	19%	11%
Victimized by their own virtual friends	78%	12%	10%
Has reported to authorities	55%	30%	15%

5. DEVELOPMENT OF CSAO

As seen in the above Section, a major cause of lack of awareness amongst students was the absence of a one stop solution where all information regarding cyber safety could be found. It was also noted that the students observed difficulty connecting to a professional Cyber Expert and many were unaware of the level of vulnerability. An initiative was thereby taken by the authors of this paper to provide a single stop solution to all Internet Safety related problems. Various resources were studied in to develop the correct guidelines and resource material for the application. Some of these resources are mentioned as [3], [8], [9], [11] and [12]. A team of cyber experts was formed and student volunteers were engaged to form a mobile application providing information about various cyber threats and to bridge the gap between victims and experts and provide tools for assessing the level of vulnerability.

Workshops were also organised in schools under guidance of our cyber expert Mr.Kshitij Adhlakha for spreading awareness about the cyber laws and safety issues. Special session was conducted for Teachers from various schools from Delhi to help them in educating their students about the cyber culture in summer vacation on 6th June 2016. The soft launch of the app took place in the workshop to make people aware about the app.

The motive of organising the Cyber Security Awareness Organisation with a group of Computer Teachers, Cyber Experts and Alumni is to provide awareness to our young citizens. For this we need a tool developed for digital natives in the form they use it at maximum i.e. smart phone. This app is a guide to parents and educators, helping in all aspects. Our primary goal of the study is to provide awareness about own victimisation and to get safe in the virtual world.

We conducted a survey on 500 students after providing them awareness about victimization. The following table describes the knowledge of victims on their own victimization.

6. PROBABLE SOLUTION TO THE PROBLEM

From our study we infer that the internet usage by children and teenagers is on high side and so do concerns about their online safety. Providing a safe environment requires an in-depth understanding of the types and prevalence of online risks young Internet users face, as well as of the solutions most effective in mitigating these risks. The use of mobile devices by youth has increased dramatically in the past few years. More work is needed to understand how this shift impacts online safety, and the extent to which mobile technologies may be “deviance amplifying.” Research on ways to encourage children/youth to more proactively report these situations at their inception could be valuable in mitigating the resulting harms. More efforts are required to better understand the impact of cyber threats in role modelling appropriate online Internet behaviors. Cyber security is the mechanism that maximizes our ability to grow commerce, communications, community and content in a connected world. The Internet is a shared resource and securing it is Our Shared Responsibility. Cyber Safety begins with a simple message everyone using the Internet can adopt: STOP. THINK. CONNECT. STOP: make sure security measures are in place. THINK: about the consequences of your actions and behaviors online. CONNECT: and enjoy the Internet.

Digital natives have created a 24/7 network that blends the human with the technical to a degree, transforming human relationships in fundamental ways. They feel as comfortable in online spaces as they do in offline ones. They only know a life connected to one another, and to the world of bits being online. The near complete integration of cameras into mobile phones has led to a “selfie” culture that puts youth in an unprecedented position: they now have the power to produce their own potentially problematic content featuring images of themselves. Such content raises many potential concerns, including the possibility that shared images could later be used in exploitative ways.

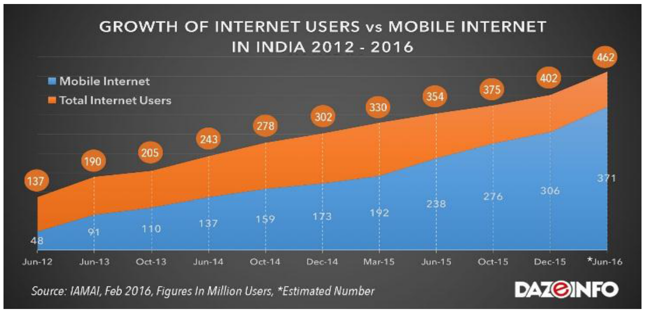
Parents are worried about the risk of abduction and encounter to the objectionable content which is available just on one click on every search engine. Their worry also include about bullying that their children may encounter online, addiction to violent video games, and access to pornographic and hateful images. Teachers worry that they are out of step with the Digital Natives they are teaching, that the skills they have imparted over time are becoming either lost or obsolete, and that the pedagogy of our educational system cannot keep up with the changes in the digital landscape. Although the issue of online privacy poses real dangers and genuine challenges, it has stolen the sleep of parents of young children. Parents and teachers need to start by putting in the time it takes to understand how the digital environment works so that they can be credible guides to young people.

Schools convey information about the Internet and impart skills related to digital safety to students in different ways, and there are lots of pedagogically sound ways to get the job done. In our school, we have arranged many workshops by cyber experts to make our children aware. Our Government is also putting lots of efforts towards digital safety for society by organizing online quizzes and competitions al national level to spread the awareness. Various campaigns are also in pipeline by the government. In the above mentioned effort of our Prime Minister towards digital awareness among young digital natives.

The fear of victimization in any form of cyber threat is a key issue for the parents and educator. Various online tools are available for parents which they can use to keep parental control over the online activities of kids. Myspace has provided a series of safety tools called “Zephyr” for parental use. The software keeps a parent up to date about the key information that their children enter into the system, including name and age. Parents can set up a kid-friendly browser, for example, to identify the user of the computer as a child to all the websites he is visiting. One such browser now available is called kidrocket.org.

Get Net Safe is a broad-based effort by the Microsoft to educate Internet users on how to protect their PCs, protect themselves and protect their families. In spite of various tools and techniques available on Internet, awareness amongst the society is the foremost requirement. To accomplish our goal of spreading awareness we conducted various workshops in our school with cyber expert.

Although many tools are available for guiding the parents and various organizations working on this issue, but there is no single tool available providing solution in cyber experts’ guidance. We developed an Android app CYBER SECURITY GUIDE as a tool for providing digital awareness acting as one stop solution to the cyber victims or the people searching for the solutions. As an IT facilitator I initiated an idea about creating this app and serve my society about the cyber security. This app is an initiative to provide the guidance to the society about cyber safety and security. This app is unique in its own terms, from providing the knowledge about threats, checking the vulnerability level, guidelines to the parents and kids, expert guidance and consultation for free. The Internet has brought untold benefits to children around the world. By June 2016, there were over 462 billion people online, which lead India to have the second-largest Internet user base in the world. In the era of the massively-available broadband Internet, cyber security and online safety is a critical issue that urgently requires a global and coordinated response. It is our duty to save our youth from the mendacious impact of cyber threat.



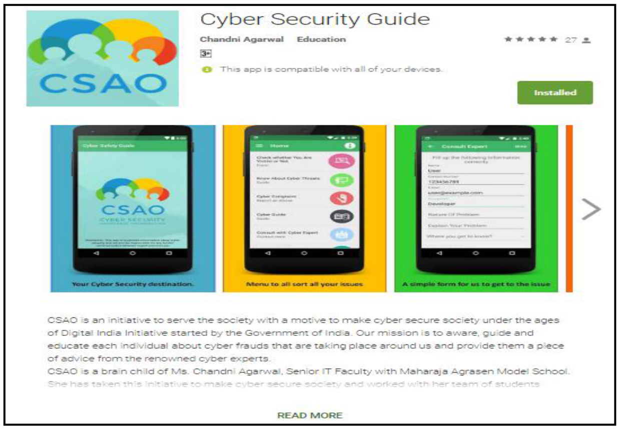
Source: IAMAI, Feb 2016, Figures In Million Users, *Estimated Number

Figure 4. Growth of internet users vs mobile users

The Internet has also raised disturbing issues, especially regarding children. Parents, guardians and educators are often referred to as ‘digital immigrants’ whereas children and young people are ‘digital natives’. The term was first coined in the book” Born Digital: Understanding the First Generation of Digital Natives”. [10]

7. SALIENT FEATURES OF CYBER SECURITY GUIDE (AN ANDROID APP)

- It provides secure login accessibility to the authorized users.
- The UNIQUE FEATURE of the App is that it provides expert help and consultation to the victim or any individual for free by the famous Cyber Experts on panel – Mr. Rakshit Tandon and Mr. Kshitij Adhlakha.
- Identify the key risks and vulnerabilities to children and young people in cyberspace.
- Create awareness of the risks and issues through guidelines and case studies.
- Initiative and aim to provide information, advice and safety tips for parents on child online protection.
- Maintains secrecy and privacy to the cyber victims.
- It provides guidelines to the parents, students about the ethical use of internet and cyber threats.
- It provides all the contact numbers of cyber cells of all the states all over India.



Cyber Security Guide

Chandni Agarwal Education

3+

This app is compatible with all of your devices.

★★★★★ 27
Installed
CSAO
Your Cyber Security destination.
Menu to all sort all your issues
A simple form for us to get to the issue

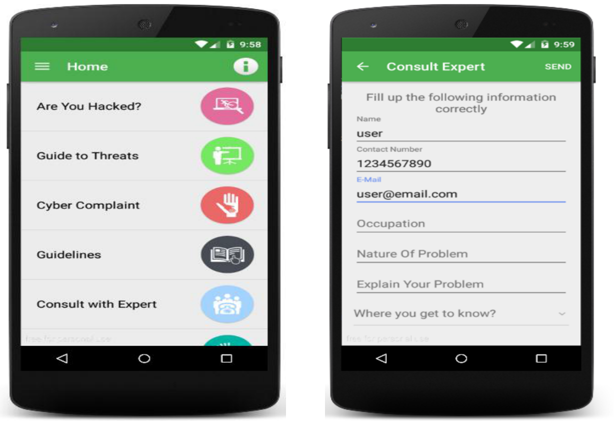
CSAO is an initiative to serve the society with a motive to make cyber secure society under the ages of Digital India Initiative started by the Government of India. Our mission is to aware, guide and educate each individual about cyber frauds that are taking place around us and provide them a piece of advice from the renowned cyber experts.
CSAO is a brain child of Ms. Chandni Agarwal, Senior IT Faculty with Maharaja Agrasen Model School. She has taken this initiative to make cyber secure society and worked with her team of students

Figure5: CSAO App at Play Store

Options available in app

- Checks the vulnerability level of victimization
- Guides about the dos and don’ts for the online presence.
- Provides the guidelines for safer usage
- Give information about the latest threats
- Also, provides the information about the latest case studies
- Cyber Experts available on panel to handle the queries sent by app on ask.csao@gmail.com

It is a complete cyber guide for the teens and society. This app is available on Google Play store for free under the category education.



Fill up the following information correctly

Name: user

Contact Number: 1234567890

E-Mail: user@email.com

Occupation

Nature Of Problem

Explain Your Problem

Where you get to know?

Figure6: App Home screen [left] and Expert Consultation Form [right].

Detailed working of the app is given on the link https://goo.gl/90r138.

8. BENEFIT TO THE SOCIETY

Children today have only experienced a world that’s cyber filled, where technology is woven into every aspect of their lives. Keeping this concept in my mind and targeting the pre-teens and teens as our key audience, for implementing this idea for a noble cause for the society I have created this cyber security app available on Google Play store for free.

How is it going to help the society

- Expert panel for the users with the option of communication. The best and unique feature of the app is to provide cyber expert help which is provided by the famous cyber experts **Mr. Rakshit Tandon and Mr. Kshitij Adhlakha**.
- A handy guide to the parents and students.
- As it is free app available on play store, everyone who has android phone with internet connection may use it.
- It provides guidelines for the parents, students and corporate, which is helpful for them to be safe on internet.
- It provides Cyber Cell helpline numbers of all the states in India. (Credits: www.infosecawareness.in)
- It also tells about the vulnerability level and do's and don'ts to the user which makes them aware.
- Anyone can seek free consultation from the eminent cyber

experts on the panel. Query can be performed by e-mail communication.

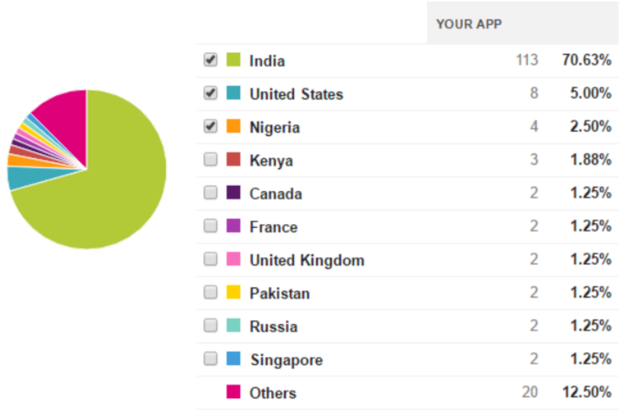
- Through case study feature, people can know about the cases going on near them.
- Parents can save their kids online.
- Many cyber-bullying cases are handled by experts, as currently no single app is providing this feature.
- The app is in simple language understandable by all.
- Instead of seeking help from unreliable resources, cyber victims can approach expert and get help.

Secrecy and privacy is maintained by the experts.

9. RESPONSE FROM APP USERS

After implementing the app with our organisation and young children of the society, we are getting good response out of it and are able to solve their queries. The stats of the application user base are given in the following figure 9.

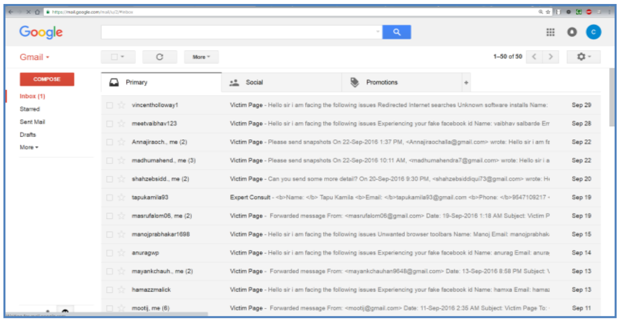
The app has been downloaded a total of 425 times with 160 currently active users (till the date of submission).



		YOUR APP	
☑	🟩 India	113	70.63%
☑	🟦 United States	8	5.00%
☑	🟧 Nigeria	4	2.50%
□	🟥 Kenya	3	1.88%
□	🟪 Canada	2	1.25%
□	🟪 France	2	1.25%
□	🟪 United Kingdom	2	1.25%
□	🟨 Pakistan	2	1.25%
□	🟩 Russia	2	1.25%
□	🟦 Singapore	2	1.25%
	🟥 Others	20	12.50%

Figure7: Number of active users in various countries

The inbox of the email id for the communication with cyber expert is given below, which shows the utility of developed app.



vincentholloway1	Victim Page - Hello sir i am facing the following issues Redirected Internet searches Unknown software installs Name:	Sep 29
meetvaibhav123	Victim Page - Hello sir i am facing the following issues Experiencing your fake facebook id Name: vaibhav salbarde Err	Sep 28
Annajiraoch., me (2)	Victim Page - Please send snapshots On 22-Sep-2016 1:37 PM, <Annajiraochalla@gmail.com> wrote: Hello sir i am fa	Sep 22
madhumahend., me (3)	Victim Page - Please send snapshots On 22-Sep-2016 10:11 AM, <madhumahendra7@gmail.com> wrote: Hello sir i a	Sep 22
shahzebsidd., me (2)	Victim Page - Can you send some more detail? On 20-Sep-2016 9:30 PM, <shahzebsiddiqui73@gmail.com> wrote: He	Sep 20
tapukamila93	Expert Consult - <b>Name: </b> Tapu Kamila <b>Email: </b>tapukamila93@gmail.com <b>Phone: </b>9547109217 -	Sep 19
masrufalom06, me (2)	Victim Page - Forwarded message From: <masrufalom06@gmail.com> Date: 19-Sep-2016 1:18 AM Subject: Victim P	Sep 19
manojprabhakar1698	Victim Page - Hello sir i am facing the following issues Unwanted browser toolbars Name: Manoj Email: manojprabhak	Sep 15
anuragwp	Victim Page - Hello sir i am facing the following issues Experiencing your fake facebook id Name: anurag Email: anura	Sep 14
mayankchauh., me (2)	Victim Page - Forwarded message From: <mayankchauhan9648@gmail.com> Date: 13-Sep-2016 8:58 PM Subject: V	Sep 13
hamazzmalick	Victim Page - Hello sir i am facing the following issues Experiencing your fake facebook id Name: hamxa Email: hamaz	Sep 13
mootj, me (6)	Victim Page - Forwarded message From: <mootj@gmail.com> Date: 11-Sep-2016 2:35 AM Subject: Victim Page To: -	Sep 11

Figure8: Inbox of the email-id receiving queries

Some of the sample case studies are as follows: (Name and location has been changed to maintain the secrecy and privacy)

9.1 Case study 1 – Cyber Bullying on Instagram

Query: Hello Sir, Somebody has uploaded my video on Instagram and have changed the page name to a vulgar name. Please help me as i am in very big trouble. The video is going viral in my college and my reputation is at stake. Please help me.

Sol: Hello. Just saw your query. Now first of all Instagram allows videos to upload only through cell phone in which there is video and not from third party devices. You uploaded the video ? Or someone who had video in his/her cell phone uploaded the video?

Query: Actually I shared my video with a page through KIK messenger for shoutout. But now name of page is changed to sizzling models and my video is posted there. I did not allow that person to upload video on the page sizzling models. Please help me i am in big trouble.

Sol: Ok. Now I understand your situation. In this case we have to report Instagram that this video belongs to you and you have not authorised anyone to use this video on your behalf. I am sending you link where you have to report. Make sure you report through your own Instagram account.

Query: I have done exactly what you said. Reported Instagram from my account only. But Instagram people said. They cannot remove the video as it has been uploaded from cell phone where the video was. And it cannot be deleted.

Sol: In this case. Let me report Instagram on your behalf. Please share your govt. issued ID proof for your authenticity. And Now I will be reporting Instagram on your behalf about copyright of video. It is your video and you are featured in it. So they will have to remove the video anyhow.

After 3 days ——

Thanks a Lot sir, the video has now been deleted. Thanks a ton for your efforts. Thanks for saving my reputation.

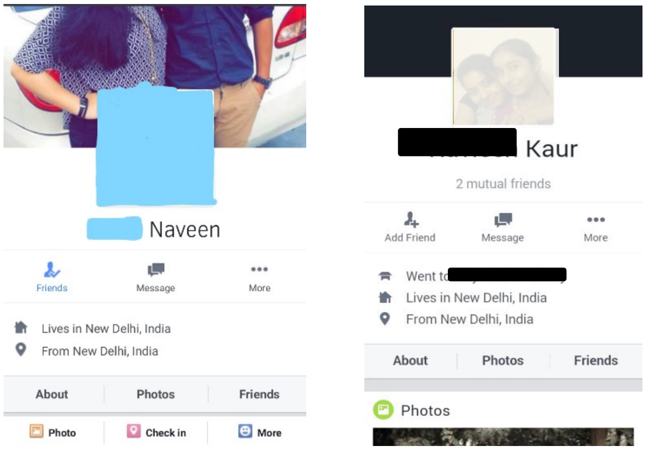


Figure9: Profile of some victims

9.2 Case study 2 – Fake Profile of a school student

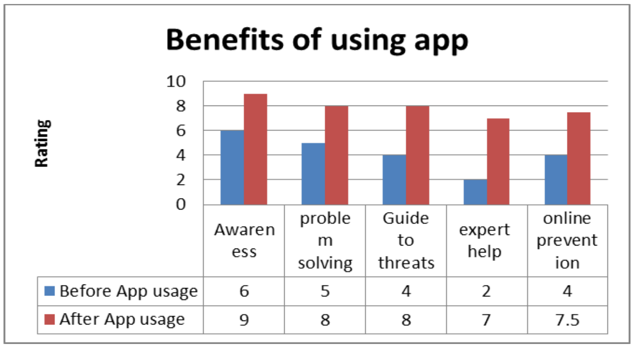
Hello sir. This side Suneha of class 12 from ABC Child Sr.Sec school XYZ place. The first session you conducted today around 8:00/8:10am,you were very influential and helpful in getting us aware, what actually Internet can do to us with your examples.I told you about my problem &you told me to converse via email. I have two accounts. First one was used by me long ago, around4/5years back for short duration. I really have forgotten my email address and password. And I think it has been hacked. Various pic that I haven't upload r just not appropriate and you told me to write this problem and you would delete my account. Another account I told you that a site naming nametests.com was used only by me rarely through Facebook and it automatically has posted it and I am really not aware that it was public or only me option and I have deactivated it last week. Does it will affect the photos/hacked. Or will it remain with sever but be safe from getting hacked?

Also, another thing I want to share is that in my phone I had an album named camera. It went off/deleted from my mobile. N suddenly it came back yesterday. I probably thought that it might have been deleted by mistake. But it came back .so according to you is it a technical problem or hacking? Bcoz it wasn't there for days n now has come back. Sir, I'm sending you the screenshot of the profile that I want to delete. Sir if u need any other details please contact me. And thank you so much for reading such a long mail. &probably it is the best session that we students have attended and this app is a wonderful platform.

9.3 Case study 3 – Fake Profile

Query: Somebody has made my fake profile on Facebook with my name and my photographs. Please help me.

Sol: Hello, Login into your Facebook profile and report fake profile by selecting option. This person pretends to be me. Fill in the form which will open after reporting and in case needed. Mail your govt. issued id proof.



	Awareness	problem solving	Guide to threats	expert help	online prevention
🟦 Before App usage	6	5	4	2	4
🟥 After App usage	9	8	8	7	7.5

Figure10: Feedback from app users

10. LIMITATIONS OF OUR TOOL

- Devices having android version less than 4.0.3 are not supported.
- Devices having RAM less than 512mb may face crashing issues.
- For updated content internet is required and application should be allowed to function in the background.
- Registration is required for using the application to filter the spammers and fake accounts.
- For registration verification through OTP is required.
- IOS and Windows devices are not supported.

11. CONCLUSION

While there are many educational programs and policy initiatives that work to promote youth/child Internet safety are needed to better inform future policies and program implementation, More research is needed to discern how best to reduce the creation, distribution, and exploitation of this content.

In the today's world of Digital citizenship, digital natives and digital migrants must learn to stay safer and more secure in their ever-expanding digital lives, including by preventing and responding to identity theft and scams, ensuring that home networks are secure, managing the security of mobile devices and teaching children to use the Internet safely, securely and responsibly.

Digital Safety is fundamental to realizing the promise of new and expanded technologies. We lead Internet-connected, digital lives. We work, learn and play online. Even when we are not directly connected to the Internet, our critical infrastructure—the vast, worldwide connection of computers, data and websites supporting our everyday lives through financial transactions, transportation systems, healthcare records, emergency response systems, personal communications and more—impacts everyone. All these evidences of online presence leads to the Internet Safety requirement. Young people around the world are spending an increasing amount of their free time connected to the Internet.

It's true that the contextual information found in cyberspace is different from the contextual information found in real space.

The home is a good place for parents to begin. They must get smarter about what their children are doing online, which need not be something their kids do by themselves in an isolated part of the home. And they need to be actively engaged with their children in a conversation about what's going on online. To make the Internet a "safe space" for their children when they are young, some parents choose to use controls such as filters to block access to certain sites and to track where their kids are going online.

Teachers and principals, too, need to step up their efforts to teach Digital Natives about the brave new world we all live in. Schools convey information about the Internet and impart skills related to digital safety to students in different ways, and there are lots of pedagogically sound ways to get the job done. In response to the Supreme Court's prior decision and in order to pass constitutional scrutiny, the scope of the new law—called the Child Online Protection Act (COPA) of 1998—was limited in several ways. As a result, an increasing number of children are accessing the Internet, creating new Opportunities for learning and sharing information or socializing throughout the world. However, this has also led to an increasing number of cases of sexual exploitation, particularly as prevention and protection measures are not systematically. The policies for cyber safety are lacking behind in our country in comparison to various others and there is a strong need to look into this matter as soon as possible. While Indian government has recently started various initiatives in this matter [6], nations like United States of America, Mauritius etc have been conducting various practises to overcome this situation from about a decade now.[7][12]

The following elements can be considered for the safe society:

- Public awareness campaign by organizing safer internet day and running child safety workshops.
- By using app as awareness and reporting tool.
- Legislation to improve child online safety
- By making policies by school authorities to make judicious use of Internet at school and home.
- By organizing quizzes and workshops at various levels
- By safeguarding the youth from ill effects of Internet.

At the last we may conclude that we all together can create DIGITALLY SAFE AND SECURE WORLD by following the guidelines of prevention from cyber threats and be alert. The Cyber Security Guide can be proven a great help to the society.

12. FUTURE SCOPE

The future scope for cyber awareness lies in developing techniques that involve the technological advancements and make use of gadgets to provide the necessary information to the potential victims, conducting exercises like Dark Screen (a city/ country wide exercise) and conducting information sharing sessions. [1]

The further plan for app is:

- To develop in different languages and for different platforms such as IOS and windows version to facilitate more people. www.csao.in the web version of app is also under process.
- To facilitate the login facility with Facebook and Gmail account.
- To attach more experts on panel.
- To organize workshop through the app registrations.
- To provide online chat with experts on the app.

The accomplishment of our primary goal to save our youth and to create a digitally safe nation is to be done by our app CYBER SECURITY GUIDE.

13. REFERENCES

[1] Cyber Security Exercises: Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events https://www.computer.org/csdl/proceedings/hicss/2004/2056/07/205670170a.pdf

[2] DebaratiHalder& K. Jaishankar, Cyber Victimization in India- A survey Report http://www.cybervictims.org/CCVCresearchreport2010.pdf

[3] Information Security , Education and Awareness http://www.infosecawareness.in/

[4] Internet Live Stats- Survey - http://www.internetlivestats.com/internet-users-by-country

[5] Mazer, J. P., Murphy, R., & Simonds, C. (2007). I'll see you on "Facebook": The effects of computer-mediated teacher selfdisclosureon student motivation, affective learning, and classroomclimate. Communication Education, http://isites.harvard.edu/fs/docs/icb.topic448497.files/Stacie%20Articles/instructor_facebook.pdf

[6] MyGov rolls out Internet Safety Campaign in collaboration with Cert-In and Googlehttps://blog.mygov.in/mygov-rolls-out-internet-safety-campaign-in-collaboration-with-cert-in-and-google-press-release/

[7] National Children's Advocacy Centre http://www.nationalcac.org/internet-safety-tips/

[8] Neil Selwyn, (2009) "The digital native – myth and reality", Aslib Proceedings, Vol. 61 Iss: 4, pp.364 - 379

[9] Palfrey & Gasser (2008)

[10] Privacy and Internet media https://www.commonsensemedia.org/privacy-and-internet-safety/age/teens

[11] Simon Johnson, Keep Your Kids Safe on the Internet (Columbus, Ohio:McGraw-Hill/Osborne, 2004), and corresponding website at http://www.keepyourkidssafe.com/. See also the website of the United States Internet Crime Task

[12] Force at http://www.usict.org/safety.asp.

[13] Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Gasser_Maclay_Palfrey_Digital_Safety_Developing_Nations_Jun2010.pdf