2012 International Conference on Computer Technology and Science (ICCTS 2012)
IPCSIT vol. 47 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V47.21

Cyber Safety Education in High Schools

Samridh Saluja[1+] , Dr. Divya Bansal[2] and Shaurya Saluja[3]

[1]The International School Bangalore, Bangalore, India
[2]PEC University of Technology, Chandigarh, India
[3]Stanford University, CA, USA

Abstract. Youth are rapidly getting exposed to latest technology, enabling them to use the internet for a variety of tasks but this also puts them at risk. A large number of 13-14 year olds are frequent online surfers and most often these children have very little education at schools pertaining to the right conduct in cyberspace. The students are not given the crucial guidelines of the internet and how to stay safe while surfing it. The same age group is constantly exposed to increasing dangers on the net. 15% of online surfers reported online harassment, 33% reported interaction with unknown people and 18% reported cyber bullying but none of these children knew where to go or what to do. Currently, none of the education boards in India have any form of cyber safety education until the 11th grade while the majority of youth internet users comprises of 9th graders unknowingly putting themselves at risk. The paper proposes a curriculum for cyber safety education in schools. The curriculum proposed covers four sections; Cyber Threats, Protecting Ourselves, Cyber Ethics and Cyber Laws. This curriculum will be made available to schools for adoption through an open source model. It can either be implemented by the school's IT teachers or by a team of committed volunteers. A crucial piece for the success of such a program is to keep the curriculum updated regularly based on feedback received and on a periodic basis as threats change and cyber safety education requirements evolve with time.

Keywords: "cyber safety" "education" "curriculum" "high schools"

1. Introduction

The youth today use the Internet, among many other things, to find and play music, watch movies, gather information for research and keep their friends posted on their social activities. Recently, the number of online teenagers engaged in content creation has been increasing. The teenagers are not only using the internet as consumers but also contribute to its vast database of blogs, pictures and videos constantly being created.

Statistics [1] from a recent study on internet studies conducted last year showed the rapid adoption of the internet by the youth and some of the dangers caused by it. Out of the surveyed youth in urban Indian schools, 84% had an internet connection at their homes. Internet use at home was highest among students between 13 and 14 years of age, with some spending as much as 8 hours online daily. Another survey by Associated Chambers of Commerce and Industry of India (ASSOCHAM) survey in 2010 revealed that about 52% of children in the 8-11 age group daily spent over five hours online - chatting and playing games. In the same age group, 30% spent between 1-5 hours a day on the net while 18% said they didn't surf daily. The usage was higher among 12-15 year olds, 58% of whom fell into the "excessive use" category. Only 10% of these children didn't surf daily and 32% spent up to five hours a day on Internet.

Among 16-18 year olds, only 4% didn't go online daily. While 56% spent more than five hours on Internet, 40% were online for less than five hours. Children of working parents were found to be more

[+] Corresponding author
E-mail address: samridh.saluja@gmail.com

addicted to the internet due to the lack of parental supervision. Although 31% of these children use the internet just for academic purposes, the remaining use it for social networking and recreational purposes. About 45% have an internet connection in their own room. 80% of the children browse internet either alone or with friends but without their parents. About 70% of the surveyed youth have online profiles on social networking sites such as Orkut, Facebook etc. Nearly 50% of these students uploaded their photos or videos on their profiles. The most undesirable cases including online harassment (15%) and unknown acquaintances (33%) are most common on social networking sites frequented by the youth. The survey also underscores the strong need for sensitizing the youth because one in ten teenagers post their phone number and information about their city and school online. 33% of the young internet users reported interaction with unknown people, although just 15% reported harassment on account of such interactions. 79% think that posting personal information online is very unsafe and that this information might be put to negative unwanted use. Of the teenagers who interacted with unknown people, 10% actually met such people in real life.

A Norton internet survey [2] found that over 7 in 10 kids in India have had negative online experiences – from exposure to nudity and violence to having a stranger try to meet with them in real life. It goes on to report that Indian kids are not following some obvious scams; 66% don’t watch out for too good to be true offers, 56% don’t always distrust online offers at first glance and 55% are not wary of too many pop-ups.

2. The Necessity Of Cyber Education In High Schools

Over the last few years, cybercrime has seen a meteoric rise. The recently released report by RSA brings out that every minute, 232 computers are infected by malware. The lightning speed at which cybercriminals develop attacks and new malware code is making it harder for global organizations to manage cyber security risk. Another survey [3] in 2009 revealed that criminal attacks using social networking sites increased by 500% between 2008 and 2009. As we see development of new technology, there is an increase in the threats and vulnerabilities. Now the development cannot be stopped but our preparation to cope with these threats can improve.

These threats pose serious risks to children since most of them are ill-informed regarding this issue. By educating kids, we are ensuring that the future generations will be safer online. There is a thin line between using the internet and abusing it and some people unknowingly cross that line. The Internet is there for use for both adults and kids so it must be seen that no matter who uses it, it shouldn't bring anyone any harm. The internet is misused by some people that indulgence in activities such as cyber bullying and the creation of fake IDs [4]. Moreover children are unaware about all of these risks and hence don't realize when they might be committing a crime by, most often, infringing the copyright law. Although illegal, this isn’t considered a crime by the teenagers today. In the study, it was also seen that children were often harassed online but didn't know what to do. These children put up their personal information and pictures in public forms without realizing that they are putting themselves in danger. In December, British security and data protection firm Sophos reported that it had conducted a probe that showed 46% of Facebook users were willing to befriend complete strangers and thus willingly hand over personal information.

Within India, it is seen that the number of households with internet has drastically increased since 5 years ago. Furthermore, the internet usage is the most among children of age 13-14. It is seen that 80% of these children browse the net without any supervision, which is a cause for concern as they may indulge in unhealthy activities. Since they spend so much time, one would think that they are completely aware of all its risks but the fact of the matter is that the teenagers do not realize the implications of their activities. It was seen that 79% of them post personal information and 33% interact with people that they haven't met in real life. 15% even reported that they were harassed online but were not aware of where to go for help. It is for this fundamental reason that cyber safety awareness needs to be looked into further.

3. The Current Level Of Cyber Education In High Schools

It is evident that countries all over the world have realised the importance of cyber education. Currently, there is a lot of cyber education related material available online [5]. These are all initiatives of the countries in response to the recent rise in cyber-attacks. It has been widely recognized as a vital requirement by most countries and has led to a large number of initiatives in making cyber safety material available online.

Essentially they all work on a voluntary basis and so aren't very viable to ensure measurable mass adoption. Cyber education needs to be institutionalized across the various segments of users. The best way for this is to do it through schools. Since everyone goes to school, this much needed education can reach a larger number of kids ensuring a wider coverage. Children are starting to use technology at a younger age and hence expose themselves to the online dangers earlier too. Schools and houses are increasingly becoming more IT enabled so it is important that the children remain safe.

To understand the current state of cyber safety education in Indian schools, a gap analysis was carried out among the prominent curriculums. A large number of students in India study in English Language based curricula CBSE – Central Board of Secondary Education, ICSE – Indian Certificate for Secondary Education and more recently with the advent of International Schools, the IB – International Baccalaureate as well. These three boards were selected for review to determine the cyber safety education coverage. There are a number of state level boards but the extent of cyber safety education in these boards is likely to be much lower than in CBSE and ICSE. We compared what is being taught and what should be taught with respect to the cyber safety topics. The results of the gap analyses are presented in Table 1 below. It is evident from the table that there is no form of cyber safety education for students below 10th grade. When a student first learns about cyber safety in 11th grade he is around 16 years old however the survey on current trends in internet usage, quoted earlier, revealed that a majority of internet users among youth are of ages 13-14. This implies that there are a large number of internet users who surf the net and use its applications without knowing all the risks involved. On top of that, in 11th and 12th the CBSE cyber safety education is taught through text books and is purely theory based, not providing the students any practical experience. This doesn't lead to sufficient exposure and isn't as relatable for the students.

CBSE, like the other curricula surveyed, does not have anything in cyber safety education prior to grade 11 which itself is a telling observation on the lack of cyber safety education at the right age. While CBSE has done well to include network security threats and attacks along with the legal issues, it does not cover modern online threats such as privacy on social networks, cyber bullying, and cyber-ethics. This current education is more focused on network security elements than on preparing students for practical, real world security issues, online behavior related dangers and how to protect themselves online.

In ICSE the coverage is limited to basic security concepts around systems controls, viruses and some fundamental coverage on how to protect using passwords and logging of actions. Once again the curriculum is not addressing essential elements relating to core concepts in cyber ethics, internet usage, social networks and what is consider illegal online. How a child needs to deal with uncomfortable situations and decisions online becomes a crucial piece which is not addressed in the curriculum.

The IB curriculum takes a data and network centric approach and provides coverage on protection of data, network security and end user management of passwords, files etc. It does not focus on the cyber behaviour elements, cyber ethics and what is considered illegal online.

Table 1. A Gap Analysis between the Prominent Syllabi with Reference to Cyber Education.

	Cyber Safety Education Coverage in Curriculum		
	CBSE	ICSE	IB
< 9th grade	Non-existent	Non-existent	Non-existent
9th and 10th	Non-existent	Non-existent	Non-existent
11th and 12th	• Network Security Concepts • Threats and prevention • Use of Cookies • Protection using Firewall • India IT Act • Cyber Law & Cyber Crimes • IPR issues • Hacking	• Security Aspects • Basic system controls - block or trap faulty data, ensure processing of data, reconstruction of files in case of disaster, prevent fraud, virus problem. • Methods of ensuring security - Password protection, Message logging	• Ensuring data security and network security, • Understand need for and use of - passwords, physical security, levels of access, marking files as read only • The need for a firewall to prevent intrusion from outside.

The poor state of cyber safety education in schools is not only an Indian problem. Michael Kaiser, executive director of the NCSA said "Kids and teens have embraced the digital world with great intensity, spending as many as eight hours a day online by some estimates, yet America's schools have not caught up with the realities of the modern economy. Teachers are not getting adequate training in online safety topics, and schools have yet to adopt a comprehensive approach to online safety, security and ethics as part of a primary education. In the 21st century, these topics are as important as reading, writing and math." [6]

4. Proposed Curriculum

It is essential that the youth are educated in a structured manner early in their lives since they are the ones who are most affected by it. This education should be integrated into students' foundational learning at school. The curriculum clearly lays out what is to be taught at what level, ensuring that children are taught the essentials at a young age and their cyber safety knowledge is further developed over time. Its main aims are to instil the right cyber behaviour & ethics in the students, make them aware of the cyber threats around them and how to keep themselves safe.

The Cyber Safety Curriculum is divided into four sections. The first section is based on Cyber Threats. When we use our computers or are connected to the Internet, we are vulnerable to many threats that could put us in danger. These threats are of many different types and have different consequences. Some decrease the computer's performance while some others steal information and give it to a third party who could misuse the same. It covers the different types of malware and computer attacks, their effect on the computer and also how their propagation. Under this there are 4 subdivisions:

Malware: Types of computer viruses with vulnerabilities, counter measures and common examples of each.

Computer Attacks: Descriptions, examples, prevention and cures for attacks like DOS (Denial-Of-Service attack), Phishing and Social engineering.

Bluetooth: This focuses on how Bluetooth works and related threats and countermeasures.

Wi-Fi: The final group covers how Wi-Fi works, Wi-Fi threats and its countermeasures.

The second section focuses on how users can protect themselves and their computers online. While on the internet, we must always be aware of what is going on in our computer and must always have control over it. No third party should be able to use our computer for their purpose. It addresses the risks of browsers and tracking cookies, the need for safer social networking and practices to follow to ensure safety online. This has 6 sections:

Browsers: The risks of browsers, their various vulnerabilities and fixes and how to browse safely.

Computer Cookies: The basic functionality of cookies, their risks and guarding against them.

Social Networking Threats: Prevention techniques and counter measures on common threats like cyber bullying, cyber harassment and cyber stalking.

Phishing and Online Transactions: Explaining how they work and also identification of phishing scams. It focuses on teaching the students what to do if they are victims to a phishing scam.

Online Gaming: talking about how it works its risks and also on how it can be made safer. The sixth part involves learning about wireless connection safety, its risks and also their mitigation.

Practices to Be Safe Online: insight into good practices that one should follow when surfing the internet. This includes an in-depth understanding of antivirus software, firewalls and patches.

The third section introduces students to the concept of Cyber Ethics. Simply put, cyber ethics is a code of behaviour for using the Internet. It is important that everyone who uses the internet have knowledge about cyber ethics so that they can keep themselves and their computer safe whenever using the internet. It provides guidance on ethical behaviour while dealing with usage of computers, exchanging information, user privacy, communications, media etc.

Part 1: It answers the essential questions such as what are cyber ethics and what is their importance. Formation of a universal list of Dos and DONTs for students to always keep in mind is also done at this stage.

Part 2: The ethics are then classified into categories. Ethics with respect to media, ethics with respect to information and case studies of past examples where bad cyber ethics have led to harming the student.

The final section provides an understanding of what is Cyber Crime and What Actions May be Considered Illegal on the Internet. While surfing on the net, it is very important that we know what is legal and what isn't. Everyone should be aware of the implications of their actions and be on the right side of the law. Some actions which some take very lightly and consider irrelevant are actually illegal. Knowing and using the net legally is a must for people of all ages. This involves educating them on the various classifications of cyber law and showing them past instances where laws were violated and the offenders were prosecuted.

Cybercrime Trends: Introduction covering the need to be aware of cybercrimes and also studying the recent trends in cybercrime.

Cyber Crime Classification: Segregation of cybercrime into categories based on two criteria. Separated by using computer as a weapon or using it as a target and also another means of separation analysing the victim/victims of the crime (society, Organisation etc.).

Cyber Laws of India: This exposes the students to the cyber laws of India and what actions are considered legal and illegal by law along with educating them on the prevention against cybercrime.

Cyber Law Case Studies: This lets the student explore the C-Files which are the Cyber Law case studies giving the children a hands on experience and letting them see what the different crimes are and also how they are solved.

5. Implementation Methodology

The curriculum would only have any effect on the children if it is taught effectively, consistently and to a large body of students. Hence to make this curriculum yield results, efficient implementation must take place. To build the right pool of trained teachers, initially teaching would be through a volunteering platform so that people from the IT and information security industry passionate about cyber safety education could be tapped in the teaching process. The curriculum and content will be dynamic and kept updated once again in an open source model. A copy of the curriculum will be put online and made available as a key resource for schools, teachers, parents and the youth and over the course of time, expect to see it evolve and improve as it gets more widely used and feedback is sought and incorporated. As newer threats emerge, the curriculum will evolve and be updated by a community eco system of practitioners, teachers and students.

6. Conclusion

Due to the continuous rise in cybercrimes students are becoming increasingly vulnerable. They are not sensitized about the various risks of surfing the net and hence end up becoming victims of cybercrime. It is also seen that children are adopting computers much earlier, putting them at risk at a young age and hence they do not understand that some of the activities they indulge in are unsafe and sometimes even illegal.

There isn’t sufficient cyber education in schools in India and as the gap analysis brought out, the current education isn’t appropriate or comprehensive enough. The employment of an apt curriculum is essential since kids should be taught about the various aspects of cyber education early on. The curriculum should ensure that cyber education is instilled at an early age in the most applicable manner. An easy to implement yet comprehensive curriculum covering cyber threats, protection techniques, cyber ethics and cyber laws catering for the their internet usage patterns of the youth has been created. Moreover, this curriculum will be taught in schools by a team of dedicated volunteers or trained teachers and will be kept relevant by regularly updating it.

7. References

[1] Current Trends In Internet Usage And Cyber Crimes Against Youth - published 2011

[2] Norton Online Family Report 2010 http://us.norton.com/cybercrimereport/promo

[3] Survey by Blue Coat Web Security Report for 2009 Trends in Cybercrime: Report- eSecurityPlanet

[4] Tribune Exclusive Report (2005, May 22) Cynthia Neff. Online harassment among teens (www.isafe.org)

[5] Survey conducted by National Cyber Security Alliance (NCSA) in 2008 (www.staysafeonline.org)

[6] 2011 edition of State of K–12 Cyber ethics, Cyber safety and Cyber security Curriculum in the U.S