Research Article

Cyber security Awareness among In-service secondary school teachers of Karnataka

K V Sridevi

Assistant Professor, Department of Curriculum Studies, NCERT, New Delhi,
Email: kvsridevi@gmail.com

Abstract

Teaching cyber security to students in schools is necessary to assist students to stay safe while using technology. Recently, a good amount of interest has been drawn towards understanding the concepts of cyber security and effort has been made by institutions to help introduce the concepts of cyber safety to the teachers. Guidelines were developed and disseminated and trainings were conducted for creating awareness about cyber security by various academic bodies like NCERT. In the present study an online survey was conducted with an objective to study the awareness levels of teachers on cyber security where in 92 secondary school teachers of Karnataka, India have participated. The findings indicate that the teachers were found to have medium level of awareness on cyber security and there is no significant difference in the cyber security awareness among the teachers with respect to gender& stream they belong to. It was found that the awareness levels on cyber security differ with respect to the age of the teachers. This study aims to open the possibilities for more research in this area in order to expand the arena for understanding the importance and usage of cyber security and how it could be implemented in the teaching environment.

Introduction

With the everyday increased usage of technology and internet in education in the form of e-learning platforms, videos and in general the changes in the society with response to online payments, applications, e-content, internet, etc., the need to protect our private data becomes a matter of concern. The manner in which we utilize the web has changed a lot in recent times. Entering our own information online to join a learning site, pursue pamphlets, web based life records, or sell utilized furniture has become the standard. Similarly, for teachers entering the data of students to calculate results or to assign tasks online on e-learning platforms has grown, along with the students' usage in general. The information created accordingly is bewildering, and expected to twofold at regular intervals. This presents as an enticing monetary benefit for programmers who can bring in cash off individuals' very own information. It has prompted numerous information penetrations as of now and there will be some more. Understanding why organizations need our information, what they do with it and the suggestions for us is new fundamental information everybody needs.

According to Data Security Council of India, India is the second most cyber attacked country in the world after

US. There are hundreds of cybercrimes that are reported on privacy invasion and data misuse, students getting on unsafe sites, etc. As a result the role of understanding how to use the internet safely is essential, thus cyber security needs to be understood and practiced to secure privacy of our own data and of the teachers as well as of the students in an educational setting. The awareness of children on using it is observed to be not adequate. As reported in a research study by Tirumala et. al (2016), a survey was conducted on students of the age group 8-12 years which consisted of questions related to the students' understanding and awareness of cyber security along with information on their internet usage. The outcome of the study indicated that cyber security awareness among the students was commonly low with the most reduced level in the 8-12 year age gathering. The students of 8-12 years age group had the option to answer just 19% of review questions. Moreover, the greater part of the students was inexperienced with basic cyber security terms and did not exhibit enough familiarity with normal cyber threats, for example, phishing. The outcome further show that most of the students didn't know about cyber security apparatuses for tablets and cell phones, which are much of the time utilized gadgets for e-learning resources.

Importance of Cyber Security

We are depending on innovations and thus creation of e material or content is being rapidly increasing. With the initiative of Digital India, today, a lot of organizations and governments store this material or content or data on Personal Computers(PCs) and transmit it across systems to different PCs. Institutions have introduced multiple e-learning resources that require the teachers and students to enter their personal information on online platforms which are prone to be hacked. Students have increased their usage of the internet, online videos and games, etc. The Internet capable technology, with its gift of resources for learning, communication, and collaboration comes with dangers of physical and emotional harm to its users, their data, and the organizations where they work and learn (Berkman Center for Internet & Society at Harvard University, 2008; National Center for Missing & Exploited Children & Cox Communications, 2006; National Cyber Security Alliance & Norton by Symantec, 2010).Information penetration has a great scope of destroying ramifications for any business. It can lead to loss of organization data and in turn the trust laid on the organization. The loss of data can cost an organization higher, especially when students are involved, it becomes all the more a sensitive deal. Going further, an information penetrate can affect corporate incomes due to resistance with information security guidelines.

Concept of Cyber Security

Cyber ethics, cyber safety, and cyber security, also known as C3, are three overlapping domains of knowledge (Pruit Mentle, 2001). Cyber ethics are the moral choices individuals make when using Internet-capable technologies and digital media; which include copyright, online etiquettes, hacking, and online

addiction(s). Cyber safety consists of the actions individuals take to minimize the dangers they could encounter when using Internet-capable technology; which include online predators and unwanted communications, viruses, and spyware. This domain also involves building an awareness of how a person's behaviour can contribute to the spread of malware and ways individuals are tricked while using Internet-capable technologies (e.g., phishing, pharming, and spoofing). Cyber security involves the technical interventions that protect data, identity information, and hardware from unauthorized access or harm. Cyber Security includes antivirus software, Internet content filters, firewalls, and password protection. Pruitt-Mentle (2008) found that cyber ethics is often seen as the responsibility of parents, whereas cyber security is the responsibility of the information technology (IT) department.

Cyber security refers to the act of guaranteeing the honesty, classification, and accessibility of data. Cyber security also includes network security, prevention of information loss, cloud security, intrusion prevention which would help in smooth digital movement. This also includes use of verification mechanisms, encryption, antivirus or malware arrangement, etc. to prevent people from cyber threats or dangers. The digital dangers include malwares, ransom ware, phishing attacks, social building, and progressed persistent threats.

In teacher education programs, pre-service teachers learn about methods to integrate technologies with content and pedagogy to improve student learning. Many presume that pre-service teachers have adequate knowledge to competently model and teach issues of safety when working with these devices as well. Pusey, P. & Sadera, A. W. (2011) investigated the current knowledge and understandings pre-service teachers have about cyber ethics, cyber safety, and cyber security topics (C3 topics) and their beliefs about their ability to teach them. The pre-service teachers were asked to rate their ability to model or teach C3 topics. The results indicated that the respondents were not prepared to model or to teach. It is reminded appropriately here that "with its gift of greater resources for learning, communication, and collaboration comes its dangers of physical and emotional harm to its users, their data, and the organizations where they work and learn Although learning institutions have been quick to profit from the Internet's gifts, they have been slow to recognize their responsibility to educate their communities about cyber ethics, cyber safety, and cyber security. This paper reports the results of a survey-based study designed to collect data regarding pre-service teacher knowledge about, and preparedness to teach, the C3 content in their future teaching. The results of this study will be the first to provide information about pre-service teacher knowledge of C3 topics and an understanding about where pre-service teachers stand in regard to teaching and modeling these topics in their own instruction. The results of this research will help teacher preparation programs to develop strategies for addressing these topics in their curriculum to better prepare pre-service teachers to integrate C3 in their

future teaching.

Pruitt-Mentle (2008) argue that C3 should be the responsibility of all, and addressing the dearth of knowledge and developing a sense of responsibility can start with teachers and teacher educators. In the past 10 years, many federal laws/Acts have been passed (in United States) that affect K-12 education.

- The Children's Internet Protection Act (CIPA) requires schools to have a clear Internet safety policy and to protect students from contact with objectionable content through the use of Internet filters.
- The Broadband Data Improvement Act (2008) requires appropriate online behaviour to be taught in schools.
- The National Educational Technology Standards (NETS) also require that C3 content be taught in schools (International Society for Technology Education, 2008).

However, these requirements are general and vague in their design and recommendations. The most significant research in this field to date is the C3 Baseline study conducted with in-service teachers (Pruitt-Mentle, 2008). This large-scale study suggests that many schools, school systems, and districts across the laws and standards ensuring covering C3 content by addressing only plagiarism and cyber bullying (Pruitt-Mentle, 2008). The C3 Baseline Study provides researchers a glimpse at C3 content integration that can be used for future comparisons with in-service teachers (Pruitt-Mentle, 2008). However, at the moment, we know very little about how colleges of education are preparing pre-service teachers to fill their obligations to professional standards and legal requirements related to the C3.

Research studies indicate that malware, plagiarism, privacy, and the protection of identity data are some of the many issues confronted be school children (Berkman Center for Internet & Society at Harvard University, 2008; Lenhart, 2010; Lenhart, Ling, & Campbell, 2010; West, 2009). In a recent study, Cranmer and Selwyn (2009) evidenced that, children in the age group of 7-11years lack a fundamental understanding of the risks to their personal safety and data. Further many researchers (Cranmer & Selwyn, 2009;LaRose, Rifon, & Enbody, 2008; Sharpies, Graber, Harrison, & Logan, 2009), express an urgent need to help build student's ability to use Internet-capable technology in a more safe, secure, and ethical way. According to Pruitt-Mentle (2008), this cannot be done with the current C3 knowledge and confidence level of many in-service teachers.

In the similar lines, in India, The National Cyber Security Policy was developed in 2013, which is a policy framework by Ministry of Electronics and Information Technology (MeitY) which aims to protect the public and private infrastructure from cyber-attacks, and safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This is basically to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and

minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation. Various organizations like National Cyber security Association of India, CDAC, Cyber Peace Foundation, Data Security Council of India, etc. have been working in creating awareness on cyber security for various stake holders at various levels. In the field of Education, Ministry of Home Affairs (MHA) developed a Handbook for Adolescents/Students on Cyber Security, and recently NCERT (2018) came out with Cyber safety guidelines for schools. These guidelines were disseminated and were used in their in-service training programmes.

Role of Teachers

The COVID-19 lockdown has forced the schools and universities to close and had to go for remote or online learning. The closure has placed unprecedented challenges on governments, institutions, teachers, parents and care givers around the world. With the development of ICT in education, online video-based courses, e-books, simulations, models, graphics, animations, quizzes, games, and e-notes are making learning more accessible, engaging, and contextualized.

In the information technology era in general and in this lockdown context in specific, teachers' use of cyber tools and need to be aware of cyber safety and security is necessary for educational institutions. The students are more tech-savvy than the teachers envision. While numerous grown-ups depend on the periodic instructional exercise to figure out how to utilize another program or application, students are computerized locals. They naturally realize how to utilize applications, cell phones, and online stages, since they've been utilizing them their entire lives. This implies, with the correct inspiration, the students could most likely make sense of how to hack into others records, which may include teachers also. For instance, if a student wasn't happy with the teacher's evaluation, he/she may have the option to make sense of the secret key and change an evaluation or two. Thus, the teachers need to be empowered to shield both themselves and their understudies from digital assaults.

Sometimes, students may be the offenders of cyber security issues in the classroom, however in others; they may be the people in question. While numerous youngsters can without much of a stretch learn computerized programs and may even hack data. They may not be sufficiently sharp to detect each cyber security chance that they experience. As a teacher, it is possible to legitimately secure students and encourage them about cyber security so they can all the more likely to defend themselves on the web.

Regardless of whether the students intend to or not, the students could put teachers, the school, and their other students in danger with their computerized propensities. The students are regularly getting more educated than the teachers when it comes to internet usage. They likely have the ability to utilize each element of the most mainstream online projects and advanced gadgets. This could give them a huge favourable position over the teacher in the event that they needed to hack into the records. As an

instructor, one most likely has various online records. Today, the student's marks, memos, progress reports, contacts, personal details, and another identifying information is all at risk of being exposed. The poor and disruptive network security poses a major threat to parents of school children whose personal records contain personal and sensitive information. The practical effects of these attacks require intervention or remedy to increase cyber security. The teacher has to be prepared and rather take all precautions by following security measures if the students approach all the data put away on those records. They need to be alert and prevent the misuse by students. Thus it is very essential to study in-service teachers' awareness on cyber security at secondary schools.

Objectives of the study

1. To determine the awareness levels of teachers with regard to cyber security at secondary schools
2. To study the difference in the awareness of secondary school teachers on cyber security with respect to their
    - Gender - male and female teachers
    - Teaching Experience - novice and experienced teachers
    - Streams – subjects taught
    - Age

Research Questions

1. What are the levels of awareness on Cyber Security among secondary school teachers?
2. How do gender, teaching experience, streams and age account for differences in the awareness on Cyber Security among the secondary school teachers?

Methodology

The design of the study was descriptive. A normative survey was carried out to explore the awareness of teachers on cyber security at schools. A questionnaire was formulated which consisted of multiple choice questions focussing on passwords, internet safety, cyber-attack, antivirus, threats to privacy in schools and on frequency of use, safety practices and management with the threats to cyber security at schools. Data Collection was carried out by administering the questionnaire online.

Description of the sample

92 teachers from Karnataka have participated in the survey, out of which 39 teachers were from Science stream (Science and Mathematics), 40 teachers from Arts stream (Social sciences and Languages) and 13 others (Physical education, Art). Sample comprises of 66 male teachers and 26 female teachers. Teachers of different age groups were found in the sample – 4teachers with less than 25 years; 26teachers with age in the range of 25 to 35 years; 40teachers between 35 to 45 years; and 22teachers in the range of 45 years and above.

Tools used

A questionnaire comprising of 26

multiple choice questions designed and developed by the researcher after the review of the existing guidelines on cyber safety and security prepared by various organisations. Thus prepared questionnaire was given for review to experts and tried out on a small sample of teachers. The finalised tool was administered through online mode. All the questions have only one correct answer; for each correct answer, one mark is given and for a wrong answer, zero is given. Total score for each student is calculated and set for analysis.

Findings on Awareness of teachers on Cyber security

Total score obtained by each teacher on awareness test on cyber security was tabulated. Then the average performance of the group i.e. Mean (11.73) and Standard deviation (3.13) were calculated. Based on the mean and standard deviation, the levels are fixed as Mean + SD i.e. above 14.86 as high, Mean-SD i.e. below 8.60 as low and the between range i.e. 8.60 to14.86 as Medium level of awareness.

Following the norms for the levels of awareness given above, it was found that 11(12%), 70(76.1%) and 11(12%) teachers were found to be with possess low, medium and high awareness of cyber security respectively. Majority of the male (75.8%) and female teachers (76.92%) were found to have medium level of awareness and very few male (12.1%) and female teachers (11.54%) were found to have higher level of awareness.

Table- 1: Awareness of teachers on cybersecurity – Gender wise

Gender	Levels of Awareness of Cybersecurity			
	Low	Medium	High	Total
Female Teachers	3(11.54%)	20(76.92%)	3(11.54%)	26
Male Teachers	8(12.1%)	50(75.8%)	8(12.1%)	66
Total	**11**	**70**	**11**	**92**

With respect to gender, there is no significant difference between the awareness of Male and Female teachers on cyber security, as the following table shows that t value (0.005) is not significant at 0.05 level, thus we can say that both male and female teachers do not differ in their awareness on cyber security issues.

Table- 2: t value for difference in the awareness of Male and Female teachers on cyber security

Gender	N	Mean	t-value	Significance
Female Teachers	26	11.73	0.005	0.996
Male Teachers	66	11.72		

Further it was also found that irrespective of the stream the teachers belong to, majority of them were found to possess medium level of awareness.

Table- 3: Awareness of teachers on cybersecurity – Stream wise

Streams	N	Mean	t-value	Significance
	Low	Medium	High	Total
Science & Mathematics	4(10.26%)	32(82.05%)	3(7.69%)	39
Social Science & Languages	4(10.00%)	31(77.5%)	5(12.5%)	40
Others (Physical Education, Art Education, etc.)	3(27.27%)	7(63.63%)	3(27.27%)	11
Total	**11**	**70**	**11**	**92**

In order to understand the significance of difference in the awareness of teachers with respect to stream the teachers belong to, one way Analysis of variance is carried out and the results are presented in table-4.

Table- 4: Results of ANOVA for awareness of teachers w.r.t. Stream

Categories	Sum of Squares	df	Mean Square	F	Sig.
Between groups	13.078	2	6.539	.660	.519
Within groups	881.128	89	9.900		
Total	894.207	91			

Teachers belonging to streams do not differ significantly with respect to cyber security ($F=0.660$, $p>0.05$) at 5% level of significance. Hence, the null hypothesis "There is no significant difference in the awareness of teachers on cyber security with respect to the stream they belong to" is accepted. It means that, the teachers do not differ in their cybersecurity awareness irrespective of the stream they belong to.

In order to find out whether the teachers differ in their awareness on cyber security with respect to their age, frequencies and percentages are calculated and presented in table-5.

Table- 5: Awareness of teachers w.r.t. Age

Age group of teachers	Levels of Awareness on Cyber security			Total
	Low	Medium	High	
less than 25 years	1(25%)	3(75%)	0	4
25 to 35 years	2(7.69%)	19(73.07%)	5(19.23%)	26
35 to 45 years	4(10%)	32(80%)	4(10%)	40
45 years and above	4(18.18%)	16(72.73%)	2(9.09%)	22
	11	70	11	92

Majority of the teachers were found to have medium level of awareness on cyber security irrespective of the age group. But none of the teachers from the age group of less than 25 years demonstrated high awareness, whereas

5(19.23%), 4(10%), 2(9.09%) teachers were found to have high awareness in 25-35 years, 35-45 years and 45 years and above age groups respectively. To find out whether this difference is statistically significant, One way ANOVA is carried out and the results are tabulated below:

Table- 6: Results of ANOVA for awareness of teachers w.r.t. Age

Categories	Sum of Squares	df	Mean Square	F	Sig.
Between groups	84.603	3	28.201	3.065	.032
Within groups	809.604	88	9.200		
Total	894.207	91			

Teachers belonging to different age group differ significantly with respect to cyber security awareness scores ($F=3.065$, $p<0.032$) at 5% level of significance. Hence, the null hypothesis "There is no significant difference in the awareness of teachers on cyber security with respect to their age" is rejected. It means that, the teachers belonging to different age group differ in their awareness on cyber security.

Further, to know the pair wise comparison of age with respect to cyber security awareness, Tukeys HSD post hoc procedures were followed and the results are presented in table-7.

Table- 7: Pair wise comparison of mean scores of cyber security awareness with respect to age of school teachers by Tukeys HSD post hoc procedure

Variable	Age(in years)	Less than 25	25-35	35-45	45 &above
	Mean	8.7500	12.7692	11.8750	10.7727
Cyber security awarenes	Less than 25	-	4.01923	3.12500	2.02273
	25-35	4.01923	-	0.89423	1.99650
	35-45	11.8750	0.89423	-	1.10227
	45 & above	10.7727	1.99650	1.10227	-

Interestingly from the above two tables it can be observed that overall teachers belonging to different age groups differ significantly with respect to cyber security awareness(ANOVA) but Tukeys HSD post hoc procedure after pair wise comparison of mean scores indicate that there is no significant difference in the awareness of teachers to cyber security when individually compared age wise.

Further question-wise analysis revealed that

- 64 (69.6 percent) of the participants knew how to create secure passwords taking care of different characters, length and avoiding mobile numbers and so on. But when asked how often do they use the same password for multiple accounts 37 percent and 33.7 percent teachers responded as always and

never, which indicates that many know how to create passwords but still are using the same password in multiple accounts.

- When asked "How often do you switch to incognito browsing for banking?", 37 percent of teachers responded as 'always' where as 38percent responded as 'never'. Further 39 percent prefer to use auto fill-in mode for apps such as paypal, paytm, google pay etc. only 10percent avoid doing it.
- 73 (79.3percent) of teachers knew that when they get a new PC, which has anti-virus software already installed, it is safe to use the internet by making sure that both anti-virus software and operating software are up to date, whereas some (8 (8.7 percent) still believe that the software that come inbuilt are obviously reliable. There was a mixed response on the updating of anti-virus software from the teachers, some 25 (27.2 percent) teachers were of opinion that when the system gets slow then it has to be updated. 78 percent of the teachers expressed that if antivirus software detects virus, then they delete that file permanently and 13percent of them treat that file through antivirus.
- Only 49 (53.3percent) of the teachers could make out that safe websites among the given and were able to differentiate https & http, whereas the others were not able to identify which one among them are safer to use while browsing. 60percent of the teachers were aware that before downloading any application one must check for the reliability of the resource.75 (81.5percent) of the teachers were aware that empty company messages of mails are threat to their devices but only 60 out of them knew the reason that they may have attached viruses.
- 74 (80.5percent) of them were aware that downloading applications from a third party website harms device, out of which 56 (60.9percent) knew the reason as they need to give access for the application to work whereas the remaining teachers were of the opinion that the application is not from the authentic webpage
- Very few participants 16 (17.4percent) were aware that when a system becomes a target of a cyber-attack one can access someone's computer and lock the user's personal files and data, many of them 72 (78.3percent) were under the impression that they can access only data available on the system. Only 45 (48.9percent) of the teachers knew that question papers saved in their phone can be leaked without their notice when the phone is hacked and others were not aware of it.
- 86 (93.5percent) out of 92 teachers were aware that one must take backup and erase data before giving a PC for repair.62 (67.4percent) teachers were aware that updating OS regularly help the devices away from viruses and hacking. Others were not aware of it. Further Very few teachers i.e. 19 (20.07percent)

were aware of the procedure to be followed when the phone is lost. Others were not sure of it. 40 (43.5percent) teachers expressed that leaving laptop on sleep mode while it is connected to internet threat as it is easy for the hackers to get access, others believed that nothing will happen. 83.7percent of them said that it is not safe to leave applications running on the background where as the remaining teachers contradicted on this opinion. Majority of the participants (70.7percent) of the study indicated that the temporary files are to be regularly removed whereas 35percent of them felt that they need to remove them only when the disc is full.

- Only 33.7percent teachers were aware of free and open softwares and operating systems like Ubuntu where as others were not at all knowing about it. They even believe that free wares are best to use.
- When asked "How often do you give permissions to all the apps to access your device's information after checking their privacy policy", 28.3percent, 13percent, 25percent, 5.4percent. 28.3 percent of teachers responded always, often, sometimes, rarely and never respectively. Out of 92, only20(21.7percent) teachers were aware that using GPS facility on phone for apps such as maps or social media is threat to them and others hardly know about it.
- 35.9percent of the teachers change the passwords of the computer promptly where as others hardly change. Further, 44.6percent of the teachers never connect to public WiFi by turning on the safety features where as others i.e. 26percent of them always turn on safety features.

Discussions

ICT and digital education has become an integral part of almost everyone's life. Although it provides immense opportunities, one should be aware of the associated risks too. As children need to utilise new technologies day by day, it is inevitable to keep themselves and the data safe and secure. In this regard the teachers' efforts are of utmost importance when it comes to educating the students for cyber safety and helping them use the internet safely. With the increase in e-learning initiatives into the education system, it has become necessary to create awareness about cyber threats as well as possible approaches to overcome them. Creating cyber security awareness among students especially for primary and secondary school is of great importance in the era of e-learning, e-commerce, e-medicine, etc. Thompson et. al. (2018), points out the misconceptions students have with regard to cyber security and how this affects their safety on the internet. Teachers can play a great role to eradicate their misconceptions and help the students use the internet safely and handle cyber threats. The results further suggest that the majority of teachers lack an understanding of the importance of cyber security and hence are not able to practice the same in their daily school routine, may it be

in maintaining the personal computers at schools or home. The Present study also witnessed similar findings where in the teachers have moderate awareness on cyber security at schools. These findings were in consonance with the study conducted by Baris Sezeret, et. al (2015) found that the teachers had an average level of awareness on cyber bullying, in general and they differ in their awareness with respect to ranch, gender and frequency of internet use. Similarly a study conducted on pre-service teachers in Haryana by Taruna Malhotra and M Malhotra (2017) evidenced that most of them have comparatively moderate awareness level of cybercrimes. Interestingly the qualitative analysis of the data also gave a clear picture that even though the teachers were aware of certain aspects like safe websites, do's and don'ts they were not applying them when it comes to utility. As no one can afford an attack it is essential to develop awareness among teachers and students on cyber safety and cyber security and motivate them to apply in their daily life situations.

References

BarisSezer, RamazanYilmaz, FatmaGizemKaraoglanYimaz (2015). Cyber bullying and teachers' awareness. Internet Research, Retrieved from https://scholar. google. co.in/ scholar?q=cyber+security+awareness+among +teachers&hl =en&as_ sdt=0&as_vis=1&oi=scholart#d=gs_qabs&u=%23p

Children's Internet Protection Act, Pub. L. No. 106-554. (2000).

Cyber space Policy Review. (2009, March 7). Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Cranmer, S., & Selwyn, N. P. (2009).Exploring primary pupils' experiences and understandings of 'e-safety.' Educational Informational Technology, 14, 127–142.

Gorman, B. (2019). Teacher's Guide to Cyber security – Everything You Need to Know in 2019

LaRose, R., Rifon, N., &Enbody, R. (2008).Promoting personal responsibility for Internet safety. Communications of the ACM, 51(3).

Lazarinis, F. (2010).Online risks obstructing safe Internet access for students. Electronic Library, 157–170.

Lei, J. (2009). Digital Natives as preservice teachers: What technology preparation is needed. Journal of Computing in Teacher Education, 25(3), 87–97.

Lenhart, A. (2010, November 9). Teens and mobile phones: Exploring safety issues as mobile phones become the communication hubs for American teens. Retrieved from Pew Internet & American Life Project at http://www.pewInternet.org/Presentations/2010/Nov/fosi.aspx

Lenhart, A., Ling, R., & Campbell, S. (2010). Teens, adults & sexting: Data on sending and receipt of sexually suggestive nude or nearly nude images by American adolescents and adults. Retrieved from Pew Internet & American Life Project at

http://www.pewInternet.org/Presentations/2010/Oct/TeensAdults-and-Sexting.aspx

Ministry of Home Affairs (MHA) (2018) Handbook for Adolescents/Students on Cyber Security https://ciet.nic.in/upload/cyber%20Safety%20Final%2031-10-2018.pdf

NCERT (2018) Cyber safety guidelines https://ciet.nic.in/upload/cyber%20Safety %20 Final%2031-10-2018.pdf

National Cyber Security Policy (2013) Department Of Electronics & Information Technology, Government of India. 1 July 2013. Retrieved 21 November 2014, https://meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

NCERT(2015). Be Safe in Cyber World, Do's and Don'ts for Teachers, Central Institute of Educational Technology, NCERT, New Delhi.

Pruitt-Mentle, D. (2008). 2008 National cyber safety, cyber security, cyber ethics baseline study. Retrieved from Stay Safe Online at http://staysafeonline.mediaroom.com/index.php?s=67 item=44

Pruitt-Mentle, D. (2000). The C3 framework: Cyber ethics, cyber safety, and cyber security implications for the educational setting. Retrieved from http://knowwheretheygo.org/static /content/MATRIX.pdf

Pusey, P. & Sadera, A. W. (2011). Cyber ethics, Cyber safety, and Cyber security: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Journal of Digital Learning in Teacher Education, Volume 28 Number 2*

Taruna Malhotra & M Malhotra (2017).Cyber crime awareness among teacher trainees, Scholarly Research Journal for Interdisciplinary studies, 4(31) 5249-5259.

Teens, Social Media & Technology (2018). Survey conducted from March 4- April 10, 2018.

Thompson, Julia D., Herman, Geoffrey L., Scheponik Travis,Oliva Linda, Sherman, Alan; Golaszewski, Ennis; Phatak, Dhananjay; and Patsourakos, Kostantinos (2018) "Student Misconceptions about Cyber security Concepts: Analysis of Think-Aloud Interviews," Journal of Cyber security Education, Research and Practice: Vol. 2018 : No. 1 , Article 5. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/5

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016).A survey on internet usage and cyber security awareness in students.2016 14th Annual Conference on Privacy, Security and Trust (PST). doi:10.1109/pst.2016.7906931