Learning Community: 10(1): 17-27, April 2019

Cyber Crime Awareness among Student-Teacher of B.Ed in Relation to Internet Usage

Yodida Bhutia and Evahunlang R Passah

[1]Department of Education, Sikkim University, Gangtok, Sikkim, India
[2]Department of Education, North-Eastern Hill University, Shillong, Meghalaya, India

*Corresponding author: yodidabhutia@gmail.com

ABSTRACT

The use of technology in the field of education has become a necessity. Computers have become a blessing to the modern educational system. Computers are being use in the education system in the management process, administrative process and in the teaching learning process. Both teacher and students are seen using the computer for their personal and academic works. Teachers and students have access to the internet through computers which are available in schools and colleges or through personal computers or through smart phones. Teachers and students can use these information to complete assignments, project, to gain better understanding on the subject matter, to publish papers and research works and share information. The study used descriptive survey method. The sample of 75 student teachers from BEd colleges of Shillong was randomly selected. The study found that the locale and having computer have impact on cyber crime awareness. There is a relation between the browsing period and cyber crime awareness among student teachers of Shillong.

Keywords: Cyber crime, Student teacher, computer usages

The Information Technology Act, 2000 states that cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information in fracture, military and government in a manner that makes it difficult to draw boundaries among these different groups. Cyberspace is vulnerable to a wide variety of incidents, weather intentional or accidental, manmade or natural, and the data exchange in the cyberspace can be exploited for nefarious purposes by both nation-state and non-state actors. Cyber threats to individuals, businesses, and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phones, compromised digital certificates, advanced persistent threats, denial of service, bot net, supply chain attacks, data leakage etc.

Chaubey (2013) stated that cyber crime is a term used to broadly describe criminal activity in which computer or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computer or networks are used to enable the illicit activity. Cyber crimes are committed while in cyberspace. They include cyber terrorism, intellectual property infringement, hacking, industrial espionage, online child exploitation, internet usage, policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more. The Information Technology Act, 2000, does not define the term "cyber crime". Cyber crime can generally define as a criminal activity in which information technology systems are the means used for the commission of the crime. Cyber crime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber crime was broken in to two categories and defined thus:

Cyber crime in a narrow sense (computer crimes): any illegal behavior directed by means of electronic operation that targets the security of computer system and the data processed by them. Cyber crime in a broader sense (computer related crimes): any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or disturbing information by means of computer system or network.

There is a different between cyber crimes and computer crime as explain by Fatima (2011). The words "cyber crime" and "computer crime" are used interchangeably in common parlance. The word "computer crimes" has wider ambit as it entails not only crimes committed on the internet but also offences committed in relation to or with the help of computers. Doon B. Parker distinguishes between the concepts of computer crime, and gives the definition of the term in the following words.

Classification of cyber crimes

Ahmad (2011) stated that cyber crimes have been classified on the basis of the nature and purpose of the offence and have been broadly grouped into three categories depending on the target of the crime. The most comprehensive classification of computer crimes has been given by David L. Carter who classifies computer- related crimes into three broad categories:

1. Where computer is the target of the crime.
2. Where computer facilitate the commission of crime.
3. Where computer is incidental to the crime.

1. Computer as a Target of the crime

This category of computer crimes aims at damaging computer system or stealing valuable information stored on the system and includes:

- Sabotage of computer and computer systems or computer network
- Theft of data/ information
- Theft of intellectual property such as computer software
- Theft of marketable information
- Blackmail based on information gained from computerized files such as medical information, personal history, sexual preference, financial data etc.

2. Computer as an Instrument of crime

The computer crimes falling into this category use computer as a medium for commission of offences. The computer programmes are manipulated to defraud others.

- Fraudulent use of Automated Teller Machine (ATM) cards and accounts.
- Credit card frauds.
- Frauds involving electronic fund transfers.
- Frauds involving stocks transfers.
- Frauds related to e-commerce.
- Telecommunication frauds.

3. Computer as Incident to the crime

The diverse application of internet made it incidental to the crimes that may be classified into two categories:

1. Internet crimes.
2. Web based crimes.

Cyber crimes is growing at a fast rate as these crime cannot be detected instantly, cyber crimes can be committed from anywhere at any time. Some of the cyber crime has not even been identify by the law maker. Chaubey (2013) has classified cyber crimes as per the Information Technology Act which are as follow:

(a) Hacking

Hacking is usually understood to be the unauthorized access of a computer system and networks.

According to section 66 of the IT Act whoever with the intent of cause or knowing that is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(b) Tampering with Computer source Document

According to section 65 of the IT Act whoever knowingly or intentionally, conceals, destroys, alters or cause another to conceal, destroy and alter any computer source code used for a computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupee or both.

(c) Publishing of Information, Which is Obscene in Electronic Form

Section 67 of the Information Technology Act, 2000 take care of this crime as under: "whoever publishes or transmits or cause to be publish in the electronic form, any material which lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt person who are likely, having regards to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punish on first conviction with imprisonment of either description for a term which may exceed to five year and with a fine.

(d) Breach of Confidentiality and Privacy

Any person who secure access to any electronic record, book, register, correspondence information, document or other material without the consent of the person concerned or disclose such any electronic record, book, register, correspondence information, document or other material to any other person shall be liable to be punished under the Information Technology Act, 2000.

(e) Child Pornography

Child pornography refers to images or films and, in some cases, writings depicting sexual explicit activities involving a child. Abuse of the child occurs during the sexual acts which are recorded in the production of child pornography. Child pornography is a part of cyber pornography but it is such a grave offence that it is, individually also recognized as a cyber crime.

(f) Denial of Service (DoS) Attack

Fatima(2011) has also emphasize that Orchestrated torrents of electronic traffic that overwhelm computers, commonly known as Denial of Service (DoS) attack, are used by cyber terrorist to jam computers. DoS attack have become grim facts of life. Potential attackers troll the internet looking for vulnerable websites. First they launch a mini attack and then they send an email to desired destination taking responsibility for the attack, threatening to mount a large attack in case the digital ransom asked for is not paid. The result is down website and a total blockage of the system. A DoS attack is characterised by an explicit attempt by attacker to prevent legitimate users of a service from using that service.

There are various cyber crimes other than those mentioned in Information Technology Act, says Chaubey (2013) which are such as Forgery, Email bombing **,** Trojan attack, Salami Attack, Data diddling, Cyber stalking, Email spoofing , internet time theft , Web jacking, Financial Crimes and Cyber squatting.

Need of the study

The internet may have proved to be a boon for the educational system but it has its dark side too. Teachers and especially students spend hours on their computer surfing the net. The internet provide a platform for interaction with the existence of social media, easy shopping and banking facilities with the online services being provided. These services attract many and at times they become an obsession and people become addicted to it. The new generation students are more into technology, they are aware of the different and new technology which are in the market. They have knowledge on their usage and can easily operate them.

On the other hand our teachers are seen to have less knowledge about the new technologies and at times are unable to even operate them. Many teachers are unwilling or do not make efforts in learning or using the computers or the internet. In this new era where the computers and the internet are ruling it is important for our teachers to develop an interest in learning about them. Teacher must be aware of the Do’s and Don’ts of the computer especially while using the internet. A teacher needs to be aware of what is right and what is wrong while surfing or using the internet. Once a teacher is aware of what is to be accepted and what is to be avoided she will not only be able to help her fellow colleagues but she will be able to make the students aware on how to be safe on the internet.

Cyber crimes are committed consciously or unconsciously. It is important that the per service and in service teacher trainees are well aware of what can lead to cyber crimes and how they can be avoided. Awareness of cyber crimes among the teacher trainees will enable them to be safe and also protect their students from the web of cyber crimes. Teacher needs to be aware of the different crimes that exist on the internet as these crimes are not always detectable. Many people are falling prey to the criminal activities being done through internet via different devices to it. Teacher awareness about cybercrime will help to educate others in the society about the different crime.

Objectives of the Study

- To study the cyber crime awareness among B.Ed student-teacher.
- To study the differences in cyber crime awareness between B.Ed student- teacher of different method papers.

    - science and social science.
    - science and language.
    - social science and language.
- To study the differences in cyber crime awareness between B.Ed student- teacher of rural and urban area.
- To study the differences in cyber crime awareness between B.Ed student-teacher having own personal computer and not having own personal computer.
- To find out the cyber crime awareness of B.Ed student-teacher in relation to the browsing period.

Hypotheses

1. H0- There is no significant difference in cyber crime awareness between B.Ed student- teacher of science and social science method paper.
2. H0- There is no significant difference in cyber crime awareness between B.Ed student- teacher of science and language method paper
3. H0- There is no significant difference in cyber crime awareness between B.Ed student- teacher of social science and language method paper.
4. H0- There is no significant difference in cyber crime awareness between B.Ed student- teacher of rural and urban area.
5. H0- There is no significant differences in cyber crime awareness between B.Ed student-teacher having own personal computer and not having own personal computer.
6. H0- There is no significant relation between cyber crime awareness and brossing period among B.Ed student-teacher.

Research Design

For the present study Descriptive Research method has been used. The Population in this study involved the B.Ed trainees of Meghalaya. As per the list obtain from the Principles of the B.Ed Collges the total number of B.E trainees are 50 in 3 colleges and Don Bosco College of teacher education has a total number of 100 students. The total sample for the present study is 75 B.Ed students teachers. For the present study simple random sampling has been used. Cyber Crime Awareness Scale developed by S. Raja Sekar (2011) was used for the study.

RESULTS

Differences in cyber crime awareness between B.Ed student- teacher of science and social science Hypothesis One- Ho- There is no significant difference in cyber crime awareness between B.Ed student-teacher of science and social science method paper.

Table 1: Difference in Cyber Crime Awareness between B.Ed student- teacher of Science and Social Science method paper

	Method Paper	N	Mean	Std. Deviation	„t"	Significance
Cyber Crime Awareness	Science	9	140.56	8.560	2.47	Significant at 0.05
	Social Science	42	132.55	10.032		

It was found that the cyber crime awareness among Science B.Ed student-teacher is higher (*M* = 140.56, *SD* = 8.560) as compared to social science B.Ed student-teacher (*M* = 132.55, *SD* = 10.032), *t* (58) = 2.47, *P* = 0.05. The table shows that there is a significant difference between the mean scores of science B.Ed student-teacher and social science B.Ed student-teacher in cyber crime awareness. Thus, null hypothesis "There is no significant difference in cyber crime awareness between B.Ed student-teacher of science and social science method paper" was not accepted at 0.05 level. The reason could be that science student-teacher are more engage in computer technology than social science B.Ed student-teacher.

Differences in cyber crime awareness between B.Ed student- teacher of science and language

Hypothesis Two-Ho-There is no significant difference in cyber crime awareness between B.Ed student-teacher of science and language method paper.

Table 2: Difference in cyber crime awareness between B.Ed student- teacher of science and language method paper

	Method Paper	N	Mean	Std. Deviation	„t"	Significance
Cyber Crime Awareness	Science	9	140.56	8.560	-0.57	Significant at 0.05
	Language	19	143.26	16.414		

It was found that the cyber crime awareness among Language B.Ed student-teacher is slightly higher (M = 143.26, SD = 16.414) as compared to Science B.Ed student-teacher (*M* = 140.56, *SD*=8.560), *t* (28) = 0.57, *P* = 0.05. The table shows that there is no significant difference between the mean scores of Language B.Ed student-teacher and Science B.Ed student teacher in cyber crime awareness. Thus, null hypothesis, "There is no significant difference in cyber crime awareness between B.Ed student- teacher of science and language method paper" was accepted at 0.05 level. Although the significant different is small the reason being could be that science B.Ed student-teacher make more use of technology in their field than the language B.Ed student-teacher.

Differences in cyber crime awareness between B.Ed student- teacher of Social Science and Language

Hypothesis Three. Ho- There is no significant difference in cyber crime awareness between B.Ed student- teacher of Social Science and Language method paper.

Table 3: Difference in cyber crime awareness between B.Ed student- teacher of social science and language method paper

	Method Paper	N	Mean	Std. Deviation	„t"	Significance
Cyber Crime Awareness	Science	42	132.55	10.032	2.63	Significant at 0.05
	Language	19	143.26	16.414		

Table 3 shows that the cyber crime awareness among Social Science B.Ed student-teacher is lower (M=132.55,SD=10.032) as compared to Language B.Ed student-teacher (*M* = 143.26, *SD* = 16.414), *t* (61) = 2.63, *P* = 0.05. There is significant difference between the mean scores of Social Science B.Ed student-teacher and language B.Ed student-teacher in cyber crime awareness. Thus, null hypothesis, "There is no significant difference in cyber crime awareness between B.Ed student- teacher of Social Science and Language method paper" was no accepted at 0.05 level. The reason being could be that B.Ed language student-teacher might have learned about cyber crime from newspaper, television or through their mobile internet.

Differences in cyber crime awareness between B.Ed student- teacher of Rural and Urban area

Hypothesis Four-Ho- There is no significant difference in cyber crime awareness between B.Ed student-teacher of rural and urban area.

Table 4: Differences in cyber crime awareness between B.Ed student- teacher of rural and urban area

	Location	N	Mean	Std. Deviation	„t"	Significance
Cyber Crime Awareness	Rural	24	129.63	10.34	3.72	Significant at 0.05
	Urban	46	140.07	12.52		

Cyber crime awareness among Rural B.Ed student-teacher is found to be lower (*M* = 129.63, *SD* = 10.341) as compared to Urban B.Ed student-teacher (*M* = 140.07, *SD* = 12.523), *t* (70) = -3.72, *P* = 0.05. There is significant difference between the mean scores Rural B.Ed student-teacher and Urban B.Ed student-teacher in cyber crime awareness. Thus, null hypothesis " There is no significant difference in cyber crime awareness between B.Ed student- teacher of rural and urban area" was not accepted at 0.05 level. In the light of the result the reason could be that urban B.Ed student-teacher have more opportunities and facilities in operating new technology therefore becoming more aware of cyber crimes such as hacking, industrial espionage, online child exploitation, internet usage, policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more when compared to B.ed student-teacher of the rural areas.

Differences in cyber crime awareness between B.Ed student-teacher having own personal computer and not having own personal computer

Hypothesis Five. Ho-There is no significant differences in cyber crime awareness between B.Ed student-teacher having own personal computer and not having own personal computer.

Table 5: Differences in cyber crime awareness between B.Ed student-teacher having own personal computer and not having own personal computer

	Having Own Computer	N	Mean	Std. Deviation	„t"	Significance
Cyber Crime Awareness	Yes	48	138.90	12.942	2.58	Significant at 0.05
	No	22	131.23	10.858		

Table 5 shows that the cyber crime awareness among B.Ed student-teacher having own computer is higher (*M* = 138.90, *SD* = 12.942) as compared to B.Ed student-teacher not having their own computer (*M* = 131.23, *SD* = 10.858), *t* (70) = 2.58, *P* = 0.05. There is significant difference between the mean scores of B.Ed student-teacher having their own computer and B.Ed student-teacher not having their own computer in cyber crime awareness. Thus, null hypothesis "There is no significant differences in cyber crime awareness between B.Ed student-teacher having own personal computer and not having own personal computer" was not accepted at 0.05 level. This could be due to student-teacher having own computer gets to spend more time in their own computer which enable them to access more information regarding crimes related to the web as compare to student-teacher not having their own computer.

The cyber crime awareness of B.Ed student-teacher in relation to the browsing period

Hypothesis Seven. Ho-There is no significant relation in cyber crime awareness between B.Ed student-teacher and the browsing period.

Table 7: Relation between cyber crime awareness and browsing period among B.Ed student-teacher

	Correlations		
		Cyber Crime Awareness	Browsing Period
Cyber Crime Awareness	Pearson Correlation	1	.094
	Sig. (2-tailed)		.438
	N	70	70
Browsing Period	Pearson Correlation	.094	1
	Sig. (2-tailed)	.438	
	N	70	70

The relation between cyber crime awareness and their browsing period was found to be *r* (68) = 0.44, which is positive modulate and significant. This indicate that when browsing period is increased, there is a significant increase in cyber crime awareness among B.Ed student-teacher. Thus the null hypothesis "There is no significant relation in cyber crime awareness between B.Ed student-teacher and the browsing period" is not accepted.

Suggestions to bring awareness on cyber crime among prospective teachers

1. Cyber Crime Awareness programme should be conducted in Teacher – Education Colleges to make student- teacher aware of Cyber Crimes.
2. Students-teacher should be made aware about the pros and cons of the internet.
3. Counseling for Teachers and Students in relation to the internet and its ill-effect related to it should be provided.
4. Teacher educator should have knowledge about computers, computers programmes, and various website in order to help students to be safe while using the computer.
5. Computer literacy should be provided through different media especially for hacking, online child exploitation, internet usage, policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more.
6. Train personal can be invented for talk on Cyber Crime Awareness in Teacher Education Colleges.
7. Basic computer education may be made available for Per- Service and In-Service teachers.
8. Teacher and students should be given training on how to access material from the internet safely and correctly.
9. Multiple media should be used to increase awareness on Cyber crime.
10. Student- Teacher should be taught to avoid plagiarism while writing assignment and research to enable authentic work.

CONCLUSION

The study found that the student-teacher of College of Teacher Education of Meghalaya have above average Cyber Crime Awareness. However, when we analyze we found that the rural student teacher have low Cyber Crime Awareness as compare to student teacher from urban areas. The reason may be that rural student-teacher have less experience and opportunity with new technology. Student teacher having own computer are more exposed to the information on Cyber Crime Awareness. The relation between cyber crime awareness and their browsing period was found to be positive and significant. Which indicate that when browsing period is increased, there is a significant increase in cyber crime awareness among B.Ed student-teacher. The study suggested that Cyber Crime Awareness programme should be conducted in Teacher Education Colleges. Teacher educator should know about hacking, online child exploitation, internet usage, policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation. So that they do not become victim of Cyber Crime and protect the information of each individual as everyone has the right to privacy. It is important for student teacher to be aware of plagiarism as one need to have authentication for their own work and also in respect to the work of others, it has also been suggested that further research on the Awareness of Cyber Laws can be done to help combat cyber Crime. In order to keep check on cyber crime one needs to have awareness and also knowledge on the precaution of the same.

REFERENCES

Balbirsingh & Jaglan, I. 2015, Study of cyber crime awareness among perspective teachers. *Arahat Multidisciplinary International Education Research Journal*, **4**(1): 63-68.

Borase, C. 2013. Study of use and difficulties faced by the B.Ed. student's for using the internet in teaching. *Aarhat Multiplediscipinary International Educational Research Journal(AMIERJ)*, **1**(5): 36-39.

Deshmukh, J.J. & Chaudhari, R.S. 2014. Cyber crime in India scenario- a literature snapshot. *International Journal of Computing and Information Technology*, **2**(2): 24-29.

Evans, M., Maglaras, A.L., He,Y. & Janicke, H. 2016. Human behaviour as an aspect of cyber security assurance. *School of Computer Science and Informatics*, pp. 1- 22.

Gandhi, K.V. 2012. An overview study on cyber crimes in internet. *Journal of Information Engineering and Applications*, **2**(1): 1-6.

Gercke, M. 1012. Understanding cyber crime: phenomena, challenges and legal response. *Cyber Crimes*, pp. 1-366.

Goyal, M. 2012. Ethics and cyber crime in India. *International Journal of Engineering and management Research,* **2**(1): 1-3.

Hutchings, A. 2013. Hacking and fraud: A qualitative analysis of online offending and victimisation. *Global Criminology: Crime and Victimization in the Globalized Era*, pp. 93-114.

Jackson, J., Allum, N. & Gaskell, G. 2004. Perceptions of risk in cyberspace. *Cyber trust & Crime Prevention Project*, pp. 1-25. Retrieved from http://www.Ise.ac.uk.

Josephine, B. & Malathi, S. 2016. Cyber crime awareness among B.Ed student teachers. *EDU Tack*, **15**(7): 25-31.

McGuire, M. & Dowling, S. 2013. Cyber- dependent crime. Cyber crime: A review of the Evidence. *Research Report,* **75**: 1-35.

Safavi, S., Shukur, Z. & Razali, R. 2013. *Reviews on cybercrime affecting portable devices. Science Direct*, **11**: 650 – 657.

Schjolberg, S. & Hubbard, M.A. 2015. *Harmonizing national legal approaches on cyber crime. International Telecommunication Union*, pp. 1-23.

Singaravelu, S. & Pillai, P.K.S. 2014. B.Ed student's awareness on cyber crime in Perambalbur District. *International Journal of Teacher Educational Research (IJTER),* **3**(3): 37-40.

Singh, G. & Prena. 2014. Cyber crime awareness among prospective teachers in relation to stream and locale. *Edubeam Multidisciplinary-Online Research Journal*, **7**: 1-8.

Urmila, G. 2014. Awareness among B.Ed teacher training towards cyber crime-a study. *An International Journal of Educational and Social Development*, **5**(2&3): 107-117.

Yadav, S., Shree, T. & Arora,Y. 2013. Cyber crime a research paper. *International Journal of Scientific & Engineering Research*, **4**(8): 856-861.