Scholarly Research Journal for Interdisciplinary Studies,
Online ISSN 2278-8808, SJIF 2016 = 6.17, www.srjis.com
UGC Approved Sr. No.45269, SEPT-OCT 2017, VOL- 4/36
https://doi.org/10.21922/srjis.v4i36.10033

COMPARISON OF CYBER CRIME AWARENESS AMONG SCIENCE AND SOCIAL SCIENCE PERSPECTIVE TEACHERS

Anupam Bansal

Assistant Professor, KIIT College of Education, Gurugram

1. Introduction:

"Cyber crime" has been used to describe a wide range of offences, including offences against computer data and systems (such as "Hacking"), computer related forgery and fraud (such as "phishing"), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content).

The word "Cyber Crime" has been derived from the words "Cybernetic" which means the science of communication and automatic control systems in both machines and living things.

The term cyber crime was earlier known as computer crime so cyber crime is any crime that involves a computer and a network. the computer may have been used in the commission of a crime or it may be the target by 21st century, though, hardly hamlet remained anywhere in the world that had not been touched by cyber crime of one sort or another cyber crime is a terms used to broadly describe criminal activity in which computers and computer network are a tool, a target, or a place of criminal activity and include everything electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computer or network is used enable the illicit activity. According to Dr. deboraty Halder and Dr. k. Jaishankar cyber crime includes offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim directly or indirectly using modern telecommunication networks such as internet (like chat rooms, emails, notice boards & groups) and mobile phones (SMS/MMS) cyber crime is the latest and perhaps the most complicated problem of the cyber world and major concern of companies, universities & organizations, worldwide governments, police departments, intelligence units have started to react as a result the issue of safety is the centre or concern for the children and adults. Common concerns regarding safety of their internet include malicious users (spam, phishing, cyber bulling, cyber stalking etc) websites and software's. As internet usage continues to rise throughout the world, the threat of cyber crime also grows. While some of the crimes are relatively harmless others are very serious. The various crimes where computer is a tool for unlawful acts are from mobile.

Although there exist many technological solutions of safeguarding the data and computer networks but in India much needs to be done towards effective use of these technologies for safeguarding the precious data. In order to achieve this purpose it is important to be aware of cybercrime.

Toyne (2003) defines "cybercrime as computer mediated activities which are either illegal or considered illicit by certain parties and which when can be conducted global electronic network."

According to Basha (2009) CBI manual defines cybercrime as :

(a) Crimes committed by using computers as a mean, including conventional crime.

(b) Crimes in which computers are targets

So, from the information provided in definitions given above, we can conclude that the misuse of cyber-space leads to the attempt of cyber terrorism and commission of crime

1.1 (a) Who are the cyber criminals?

Mostly it has been observed that these criminals are:

(a) Children and adolescents between the age group of 6-18 years. Reason for such kind of behaviors in them is done to the inquisitiveness to know and explore the things and other reasons may be to prove themselves to be outstanding among other children in the group.

(b) The group of organized hackers, who adopt such behavior to fulfill their objectives of personal bias, fundamentalism etc.

Ex. Pakistanis are said to be one of the best quality hackers in the world and their main targets is the Indian government sites to fulfill their political objectives.

(c) The professional hackers who work for money generally employed to hack the sites of the rivals and get credible, reliable and valuable information and to detect their loopholes.

1.1(b) Now, who are the victims?

*****Mostly they are the companies who do not have any security awareness.

*The unaware individuals or don't care individuals or the innocent individuals.

*Another major victim is society as a whole.

1.2 Different types of cyber crimes

As internet usage continues to rise throughout the world, the threat of cyber crime also grows. While some of the crimes are relatively harmless others are very serious. The various crimes where computer is a tool for unlawful acts are from mobile

1.2.1 Hacking:

Hacking is the most common type of cybercrime committed across the world. In simple words, hacking is a crime which entails cracking systems and gaining unauthorized access to the data stored in them. Hacker is a person who breaks in or or trespasses a computer system.

1.2.2 Cyber Stalking:

Cyber stalking is use of internet or other electronic means to stalk someone. It is online harassment and online abuse. Mostly cyber stalking involves following a person's movement across the internet by posting threatening messages to the victim or by entering the chat-rooms frequented by the victim or by constantly bombarding the victim with the e-mails etc.

1.2.3 Virus Dissemination:

Virus is the programs which attach themselves to the computer or file and then circulate themselves to other files and to other components on a network. They usually affect the data on the computer, either by altering or deleting it.

1.2.4 Dissemination Of Obscene Material/Pornography:

Internet has provided a medium for the facilitation of crimes like pornography. Almost 50% of the websites exhibit pornographic material today. This crime includes hosting the website containing this prohibited material, use of computers for producing these obscene materials and downloading through the internet the obscene material. These obscene matters may cause harm to the minds of adolescent and to corrupt their minds.

1.2.5 Cyber Defamation:

Defamation as an act to impute any person with an intention to lower the person in the estimation of right-thinking members of the society. Cyber defamation involves use of computer or the internet as a medium to commit such crime. E.g. the e-mail account of Rohan and some mails from his account was sent to some of his friends regarding his relationship with underworld with intent to defame him.

1.2.6 Online Fruad And Cheating:

This is also a form of cybercrime. It can be in the form of credit card crime, offering jobs etc. Certain computer viruses can log keystrokes on your keyboard and send them to the hackers, who can then take your social security numbers, credit card numbers and home addresses. This information can be used by the hackers for this own means.

1.2.7 Phising:

Phising is just one of the many frauds on the Internet, Phising trying to fool people into parting with their money. Phising refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account.

1.2.8 E-Mail Spoofing:

A spoofed e-mail is one that appears to originate from one source but actually has been Sent From Another Source. This Can Also Be Termed As E-Mail Forging.

1.2.9 FORGERY

Sometimes counterfeit currency notes. Postage and revenue stamps, mark sheets etc. can be forged using sophisticated computer, printers and scanners.

1.2.10 Data Diddling:

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable. It is altering of raw data before the computer processes it and then changing it back after the processing is completed. It may lead to huge losses to the organizations.

1.3 Cyber Law In India

To further deal with the problem of cybercrime the victims can even take the help of information Technology Act, 2000. India enacted this act to regulate and control the affairs of cyber world in an effective manner. Chapter 1X of this act deals with offence/crimes along with certain other provisions scattered in this act. The various offences which are provided under this chapter are:

Tampering with Computer source documents	**Sec.65**
Hacking with Computer systems, Data alteration	**Sec. 66**
Publishing obscene information	**Sec. 67**
Un-authorized access to protected system	**Sec. 70**
Breach of Confidentiality and Privacy	**Sec. 72**
Publishing false digital signature certificates	**Sec. 73**

2. Objectives

1. To study the level of Science B.Ed. Pupil teachers.
2. To study the level of social Studies B.Ed. teachers on Cyber Crime.
3. To investigate the significance difference between Cyber Crime Awareness of B.Ed. Science and Social studies pupil Teachers.

3. Hypothesis

H01 There is no significant difference in Cyber Crime Awareness among B.Ed. Science and Social studies Pupil teachers.

4. Operational Definitions

1. **Cyber Crime: -** Computer Crime or Cyber Crime is any crime that involves a computer and a network. The term “Cyber crime” has not been defined in ant statute or Act. The Oxford Reference Online defines ‘Cyber crime’ as crime committed over the internet. The Encyclopedia Britannica defines ‘cyber Crime’ as any crime that is committed by means of special knowledge or expert use of computer technology.

2. **Stream: -** B.Ed. Pupil Teachers will be divided into two streams. Those having Science as their teaching subject will be considered as Science Pupil Teachers and those having Social studies as their teaching subject will be considered as Social Studies Pupil Teachers in the present only.

5. Methodology

5.1 Design of the Study

In the Present Study Descriptive Survey method was used.

5.2 Sample of the Study and Sampling technique

A Purposive sample of 50 B.Ed. students from self financed Education College (KIIT College of Education) of Gurugram was taken.

5.3 Tools of the Study

Cyber Crime Awareness Scale by Rajasekar (2011) will be used in the present study.

5.4 Statistical Techniques

T- Score was used to analyze the data and test the null hypothesis.

6. Analysis and Interpretation

6.1 Level of B.Ed. Science Pupil Teachers Awareness on cyber Crime.

Table 6.1

S. No.	Level of Cyber awareness	Grade	Raw score range	No of B.Ed. Pupil
1	Excellent awareness	A	>143	7
2	High awareness	B	133-142	8
3	Above average awareness	C	123-132	4
4	Moderate awareness	D	108-122	3
5	Below average awareness	E	99-107	2
6	Low awareness	F	88-98	1

6.2 Level of B.Ed. Social Studies Pupil Teachers awareness on Cyber Crime.

Table 6.2

S. No.	Level of Cyber awareness	Grade	Raw score range	No of B.Ed. Pupil
1	Excellent awareness	A	>143	5
2	High awareness	B	133-142	6
3	Above average awareness	C	123-132	3
4	Moderate awareness	D	108-122	5
5	Below average	E	99-107	4

	awareness			
6	Low awareness	F	88-98	2

6.3 H01 "Difference in Cyber Crime Awareness of B.Ed. Science and Social Studies Pupil Teachers."

Table 6.3

Variables	**N**	**t-ratio**	**Remarks**
Science Pupil Teachers	25	2.659	Significant
Social Studies Pupil Teachers	25		

Table 6.3 reveals that mean scores of B.Ed. Pupil science and Social Studies Teachers are 158.80 and 148.80 respectively. The calculated t-ratio is 2.659. The calculated t-value is significant at 0.05 level as the calculated value is greater than the tabulated value i.e. 2.01. The B.Ed. Science Pupil Teachers thus are significantly more aware about the Cyber Crime than the B.Ed. Social Studied Pupil Teachers. The significant of difference as indicated by the findings might be due to more exposure of computers to science graduates as compared to graduates from Social Science streams. The students of Science Streams most frequently use Computers.

Thus the null hypothesis H01- There is no significant difference in the Cyber Crime awareness of B.Ed. Science and Social Science Pupil Teachers is rejected

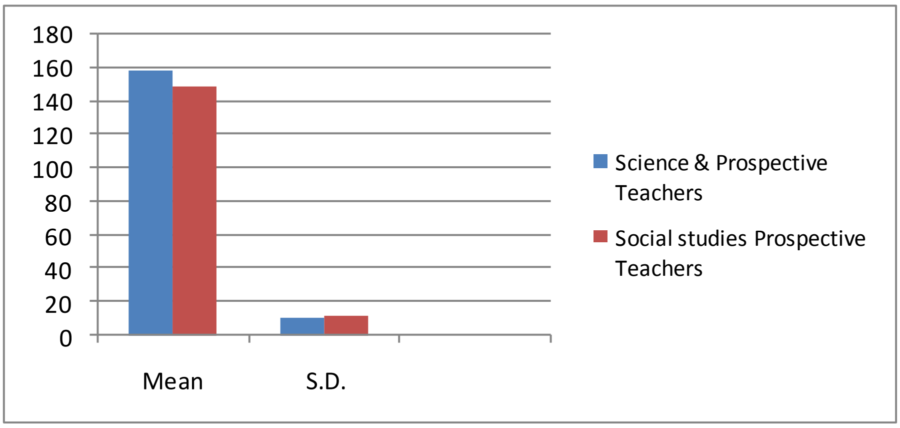

Figure 6.1 Difference in the Cyber Crime Awareness of Prospective science and Social Studies Teachers

7. Major Findings

On the basis of the result obtained in the investigation by analysis and interpretation, the following findings were drawn from sample taken in present study:

1. Level of B.Ed. Science and Social Studies Pupil Teacher's awareness on Cyber Crime.
2. There is a significant difference in the Cyber crime Awareness of Science and Social studies pupil teachers.

8. Educational Implications

Cyber Crime also called Computer Crime, the use of computer as an instrument to further illegal ends, such as committing fraud, trafficking in the child pornography and intellectual property, stealing identities, or violating privacy. Cyber Crime, especially through the internet, has grown an importance as the computer has become central to commerce, entertainment, and government. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another. The result of the study can be usefully employed in school practices.

The present study has the following educational implications for the B.Ed. trainees(Pupil Teachers)

1. It can help to know about the level of awareness towards level cyber crime in student.
2. The B.Ed. pupil teachers can tell their students about the harmful effects of using internet without sufficient preventive measure.
3. The B.Ed. pupil teachers can tell their students about safe internet browsing and protect themselves of being victims.
4. It can help in decreasing the involvement of students in cyber crime who do mistakes due to the lack of awareness towards cyber crime.
5. The students can protect themselves from hacking phishing spam identity theft etc.

9. Conclusion:

To check the cyber crime it is essential that the B.Ed. Pupil Teachers must be aware about this. The study shows that the B. Ed pupil Science teachers are significantly more aware that

B. Ed pupil Social studies teachers. It is thus suggested to the teacher evaluators and policy makers to create conducive conditions creating awareness among Social studies pupil Teachers. Creation of Cyber Crime awareness among the B.Ed. Pupil Teachers will help in the creation of cyber crime awareness among the students as these Pupil Teachers are preparing to enter the teaching profession.

Reference

BOOKS:

Babbie, Earl. The Practice of social Research. 10th Edition. Thomson, Wadsworth.

Best, J. and Khan, J. (2008). Research in Education. New Delhi: Prentice Hall of India.

Garret, H.E. (1970). Statistics in Psychology and Education. Bombay: Vakis Fetter & Simons Pvt. Ltd.

Good and Carter, V. (Ed.) (1945). New York: McGraw Hill Company.

IGNOU. (2007). MES -016 (Blocks: 1-5) Educational Research. New Delhi.

Kothari, C.R. (1990). Research Methodology - Method & Techniques. New Delhi: Wiley Estern Limited.

Koul, L. (2009). Methodology of Educational Research. New Delhi: Vikas Publication House (P) Ltd.

Mangal, S.K. (2002). Advanced Educational Psychology. New Delhi: Prentice Hall of India.

JOURNALS:

Basha, K.N. (2009). Cyber Crime. Paper presented in Seminar And Workshop On detection of cyber crime and investigation. Sardar Vallabhbhai Patel National Police Academy, Hyderabad from 20/06/2010 to 28/06/2010.

C.B.I Manual as quoted by Arpana & chauhan, M. (2012). A study regarding awareness cyber crime in Tricity. International Journal of Enterprise Computing and Business system, 2(1), 9. Available at http://www.ijecbs.com.

Rajaeskar, S. (2011). Manual for cyber crime awareness scale, CCAS-RS. Agra: National Psychological Corporation.

Sidhu, K.S. (1999). Methodology of research in Education. New Delhi: Sterling Publishers (P) ltd.

Singh, C. (2013). Awareness about cyber crime among pupil teachers of Ludhiana district. Unpublished M.Ed. dissertation, Punjab University, Chandigarh.

Dalal P. (2010). Awareness of cyber Law in India, retrieved from http://cyberlawinindia.blogspot.in/2010/05/awareness-of-cyber-law-in-india.html on September 03,2012.