



CYBER CRIME AWARENESS: A STUDY (WITH SPECIAL REFERENCE TO B.ED. STUDENT TEACHERS)

UTTAM MANDAL ¹

¹ ASSISTANT PROFESSOR, PLASSEY TEACHER TRAINING INSTITUTE PLASSEY, NADIA, WEST BENGAL.

ABSTRACT:

Communication technology has become the essential part of the computer. One can't even think about education without the use of computers, different media and internet. Internet is growing so rapidly that it has become the need of the hour. Not only students but teachers also depend on the internet for various information. As it is the law of nature that every coin has two aspects so as the communication technology has which is called cyber crime. Cyber crime is considered as criminal behaviour. Cyber crime includes many criminal activities by using internet such as programming theft, spam, hacking, and identity theft internet fraud. So it is very important for instructor students to be very careful of cyber crime occurring on the web.

According to Florida international University, "cyber crime is a criminal demonstration by methods for through on PC that happens over the web. The web has convert the hotspot for various kinds of wrong doing and various approaches to play out these violations. The kinds of cyber crime might be approximately partitioned into three classes of cyber crimes. First the web grants for the plan and upkeep of cyber crime commercial centers. Second the web has turned into a spot for the advancement of cyber criminal networks. Third the web gives a scene to tricky conduct (digital scam)."

In the present time cyber crime is one of the major problems which are spread around us like a pandemic. So it is very essential to warn B.Ed. student's teachers as well as general public about it.

KEYWORDS:

COMMUNICATION, TECHNOLOGY, CYBER CRIME, B.ED. STUDENT TEACHERS, ESSENTIAL.

PAPER ACCEPTED DATE:

10th February 2024

PAPER PUBLISHED DATE:

11th February 2024

INTRODUCTION

Cyber crime is a serious issue of present time. A big part of territory is affected by it. The biggest factor of spreading cyber crime is demonetization. Most of the cyber crimes are done through, net banking, Google pay and different sources. Most of the people are using cashless transactions after demonetization thus cyber crime is at the peak in India. More than 90% of population is depend on internet for various work so it is impossible to even think about anything without technology. Teachers, students, teacher's investigators and other all are depend on the internet for every information that is why cyber crime has got a boost. This is criminal behaviour on the web such as clandestine activities, programming theft and spreading infections. Thus, the trainers who introduce students to ICT education and skills should also be aware of the cyber crimes taking place on the web.

DEFINITION

Debarati Halder and K. Jaishankar describe about cybercrimes: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss to the victim directly or

indirectly, by means of modern telecommunication networks such as internet (networks including but not limited to chat rooms, emails, notice board and groups) and mobile phones (Bluetooth/ SMS /MMS)"

CYBER CRIMINALS

Cyber Criminals can be seen in different groups or categories. There are three categories of Cyber criminals.

1. Age group of 6-18 years old children

This is the age where hormonal changes take place and children are very curious in this age to know and investigate about everything that they should not and they indulge themselves in such activities.

2. Hackers

Such type of people creates an organised group in order to accomplish some certain goals. The reason could be to satisfy their political leanings, fundamentalism and many others.

3. Professional Hackers/ Crackers

These hackers are mainly motivated by cash. They hack the Identity of others on net and get cash. Sometimes they

remove or harm to the important information of the person whose ID is being hacked.

According to the information Technology Act,"2000 was enacted with the aim of creating and enabling environment for the commercial use of LT. The IT act describes the acts that are made punishable. Also the Indian Penal Code, 1860 This has been adjusted to includes Cyber crimes. Web related offences and offences that have been convicted under the IT Act and IPC are as follows:" Computer source government papers and tempered-section.65

Hacking with Computer Systems, score changes section.66

Publishing X- rated information -section 67

Violation of discretion and confidentiality- section 72

Publishing fake digital signature certificate-section 73

DIFFERENT TYPES OF CYBER CRIMES

1. Cyber stalking
2. Denial of Service Attack
3. Virus Attacks
4. Pornography
5. Software Piracy
6. Network Hijacking
7. Identity Theft
8. Cyber theft
9. Hacking
10. Unauthorised Access

CLASSIFICATION OF CYBER CRIMES

Cyber crimes can generally be classified into four categories:

1. Personal Cyber Crime: This type of Cyber crime targets individuals. This includes phishing, spoofing, spam, cyber stalking and more.
2. Organization Cyber Crime: The main target of organisation cyber crime is organisations. Typically, this type of crime is carried out by teams of criminals including malware attacks and denial of service attacks.
3. Property Cyber Crime: This type targets assets such as credit cards or even intellectual property rights.
4. Society Cyber Crime: This is the most dangerous form of Cyber crime as it also includes cyber-terrorism.

NEED OF THE STUDY

Inspire of having many positive aspects internet has a black side too which is called cyber crime. In present time internet provides many types of online services and other facilities. Basically these services have made us dependent on them. The new generation people teachers are very interested in technology and don't want to do anything without technology but those who are continuously working in various field using internet they must know about cyber crimes and the tricks to avoid them.

Awareness about cyber crimes among teachers trainee is extremely important because this awareness is the only solution to save themselves from the trap of cyber crime.

CYBER CRIME AWARENESS

To create awareness about cyber crime among B.Ed. pupil teachers, seminars related to the subject should be organised in teacher education colleges.

B.Ed. pupil teacher should keep telling the advantages and disadvantages of internet from time to time.

Teachers and students should be made aware of both the negative and positive aspects of the internet.

Students should be told about the ill effects of the internet.

Student teachers should be taught to be cautious while using computers and avoid working on unknown websites.

Student teachers should provide education on the use of special tools especially hacking, computer literacy through online classes.

B.Ed. pupil teachers should be made aware on topics like child exploitation, use of internet, misuse of various internet policies illegal purchase of goods etc.

B Ed. Pupil teachers should be provided information on topics related to fraud, software Piracy, virus cloning etc.

To protect B.Ed. student teachers from cyber crime activities like speeches on cyber crime alert should be organised in colleges. B.Ed. student teachers should be provided basic computer education to avoid cyber crimes.

Teachers should educate B.Ed. students on how to access material from the internet safely and correctly.

Multiple media should be used to increase cyber crime awareness among B Ed student teachers.

B.Ed. students should be asked by teachers not to plagiarize while preparing assignment research etc. to make the work original and competent.

If cyber crime awareness is compared between urban B.Ed. pupil teachers and rural B.Ed. pupil teachers, then it is found that urban students are more aware about cyber crime than rural students.

They are highly associated with technical education and remain alert about scams done on the Internet. While rural student teachers, being of simple nature, become victims of cyber crime and get trapped in the web of cyber crime and loss their money in many ways.

At present it is very essential to make rural student teachers aware about cyber crime.

To avoid frauds in the field of education and internet, there is a need to organise various types of symposiums, seminars, workshops, guest lecturers etc.

Even today, there are many parts of our nation where students are able to know the comprehensive nature of the internet due to lack of technical facilities. Nor they are able to understand cyber crime. Lack of technical education and facilities in rural areas make it difficult to make the pupil teachers learn even in their regional languages. Therefore,

it is very difficult for them to know about cyber crimes and the ideas to protect themselves from Cyber crimes. To protect such students from cyber crime it is necessary to start cyber crime awareness programs in rural areas through educational institutions, social service organisations, television and media.

When the people of entire nation will be aware about cyber crime, then the power of evil people active in the field of time will gradually become weak and the day will not be far when cyber crime will be eliminated from the society.

CONCLUSION

To conclude it can be said that cyber crime awareness is very essential in our daily life because we start our day with internet as well as end it with the same thing. Now a day's newspapers are also read on internet by us. Banking, Education, Shopping, Project works, accounting everything is done with the help of internet. But the lack of awareness against cyber crime can be very harmful and can convert our happy life into worst one. So being aware and alert is the only solution to be away from CYBER CRIME.

REFERENCES

1. Subahjit Basu (2012), "Cyber Stalking on Online" Cyber Situation in present scenario, Volume 5.
2. Antoniadou, Nofsika & Kokkinas (2013)- "Cyber bullying" National Journal of cybercrime Volume 4.
3. Bryce J Renninger (2014), "Counter Public communication on Social Networking Sites" SNS, volume2.
4. Alia Baniyaga (2017) - "Cybercrime And Cyber Personality" The Commission Of Human Rights.
5. Bijoy Saima (2017), - "Cybercrime awareness among students of Govt. Law College" Cyber Psychology, Volume 4.
6. Brijesh Singh IPS (2017) Inspector General, Cyber Maharashtra "Cyber Attacks on the Rise" Cyber Security Incidents.
7. "A Study of Awareness of cybercrime awareness of cybercrime among college Students with special Reference to Kochi" International Journal of Pure and Applied Research Volume 119, No. 16, 2018
8. Gilberto Marjano(January 2019)," Cyber Bullying And Social Networking Sites" Cyber Bolenge And Critical Importance Of Educational Resources For Prevention And Intervention.
9. Hogan (2019), Personality Types To Succeed In Cyber Security, Journals Of Cyber Crime Awareness.
10. Hogan (2019), Personality Types To Succeed In Cyber Security, Journals Of Cyber Crime Awareness.
11. Sudha Mishra (2019) "Cyber Fraud after Demonetization". National Cyber security, volume 4.