

Cyber Crime Awareness among Teacher Trainees

Sunil Kumar¹, Dr. Kuldeep Kaur Grewal², Dr. Mohua Khosla³

¹Research Scholar, Department of Education, CT University, Ludhiana (Punjab) INDIA

²HOD, CT University, Ludhiana (Punjab), INDIA

³Associate Professor, Malwa College of Education for Women, Ludhiana (Punjab)

Abstract: Cybercrime's 'definitions' are largely determined by the context in which it is used. The root of cybercrime is a small number of actions that compromise the confidentiality, credibility, or availability of computer data or systems. Beyond that, computer-related actions for personal or financial gain or harm, such as identity-related crime and computer content-related acts (all of which come under a broader definition of the word "cybercrime"), do not lend themselves easily to legal definitions of the term. The aim of this study was to look into the knowledge of cybercrime among Teacher Trainees. The study included 200 B.Ed. students from three separate education colleges in Ludhiana: B.C.M. College of Education, Malwa College of Education for Women, and Partap College of Education. There were 50 males and 150 females among the 200 B.Ed. students. The researcher developed his own scale of cybercrime knowledge. This scale has 42 sentences, 24 of which are positive statements and the other 18 are negative statements. Each claim was rated on a five-point scale. According to the findings male and urban Teacher Trainees were both more conscious about cybercrime than female and rural Teacher Trainees respectively.

Keywords: Cyber crime¹, Awareness², Teacher Trainees³.

I. INTRODUCTION

Young people are increasingly spending time online for purposes such as learning, transacting, shopping, social networking, sharing images, and gaming. While this has improved connectivity, efficiency, and entertainment, it has also made us more vulnerable to cyber-crime than ever before. According to reports cited in the International Telecommunication Union (2012), at least 2.3 billion people, or more than one-third of the world's population, had internet access in 2011. More than 60% of all internet users live in developed countries, with 45% of all internet users under the age of 25. By 2017, it is anticipated that mobile broadband subscriptions will account for nearly 70% of the global population. By 2020, the number of networked devices (the "internet of things") will outnumber people six to one, fundamentally altering existing internet perceptions. In tomorrow's hyper-connected world, it would be difficult to imagine a "computer crime," or perhaps any crime that does not involve electronic evidence linked to internet protocol (IP) connectivity. The benefits of the Internet include the ability to access a wide range of information at any time and from any location; trade and business change and growth, electronic government, e learning and education, science, entertainment, and culture, among others. The disadvantages through Internet include hacking, email bombing, unauthorized access to email accounts, data altering, salami attacks (financial crimes), service attack (service blocked)/trafficking, viruses / worm attacks, Trojan attacks / unauthorized programme, fake emails internet time theft, web jacking, blackmailing, violation of privacy, indecent mailing/ dissemination of obscene material, pornography, improper downloading of copyrighted material etc. Cybercrime's 'definitions' are largely determined by the context in which it is used. The root of cybercrime is a small number of actions that compromise the confidentiality, credibility, or availability of computer data or systems. Beyond that, computer-related actions for personal or financial gain or harm, such as identity-related crime and computer content-related acts (all of which come under a broader definition of the word "cybercrime"), do not lend themselves easily to legal definitions of the term. While firewalls, antivirus software, and other technological solutions exist to protect data and computer networks, India still has a long way to go in terms of making effective use of these technologies to protect sensitive data and fight cybercrime. Also the most experienced users of IT tools may be unaware of cyber-attacks. Along with technological advances, it is also important to be aware of cybercrime and related issues. Cyber security is determined by a user's understanding of technology and the precautions taken when using the internet, as well as the protective measures taken by the user and server systems. It has been said that the issues that have been generated cannot be solved with the same degree of knowledge that has caused them. As a result, there is a need to raise cybercrime awareness. The rising threat of cybercrime in India necessitates increased technical, behavioural, and legal knowledge, as well as appropriate education and training. According to Bhushan (2012), India's understanding of cybernetics is abysmally poor, and as a result, it has earned a reputation as a country where foreign investors can do business in cyber security, and it has been heavily investing in cyber security. Pandey (2012) concluded that a lack of internet knowledge and a poor level of internet security is rapidly turning Indore1 into a cybercriminal haven. Since people are unaware of the rapid changes in the cyber world,

the number of cybercrimes has steadily increased. The growing reliance of ordinary citizens on cybernetics without adequate protection has made cybercriminals' job easier. Indore has become more vulnerable to cybercriminals due to a lack of experts and cyber sleuths, according to the researcher. According to Nappinai (2010), many cases of cybercrime are not prosecuted due to a lack of understanding among both victims and enforcement agencies about the applicability of general laws to cybercrime. According to Saxena, Kotiyal and Goudar (2012), constructive government actions and increased involvement of the educational system in the cyber security awareness approach may contribute to a more secure country. According to Seth (2007), India can effectively combat the problem of cybercrime by raising awareness and providing training on the issue, as well as taking enhanced technical and legislative measures to further strengthen the IT laws and compliance system. Kumar (2013) stressed the importance of cyber laws and information security, online awareness programs, cybercrime cells, concept inclusion in the syllabus, media in creating awareness, and academic libraries in guiding their user group to avoid white collar crimes. According to Mehta and Singh (2013), there is a noticeable gap in knowledge levels between male and female users of internet services, with male netizens becoming more aware of Indian cyber laws than their female counterparts. Singaravelu and Pillai (2014) examine B.Ed. students' knowledge of cybercrime. In the current study, a normative survey approach was used. The sample of 200 B.Ed. students studying in the College of Education in the Perambalur district of Tamilnadu, India, was chosen using the cluster sampling technique. According to the study's findings, the majority of B.Ed. students have a poor level of knowledge about cyber forums. To produce cyber age students, it is suggested that B.Ed. students balance cyber technology policy and preserve the order of online law. Institutions are required to start a cybercrime awareness programme for students.

Objectives: The following were the objectives of the study

To study the cybercrime awareness among Teacher Trainees.

To compare the cybercrime awareness among male and female Teacher Trainees.

To compare the cybercrime awareness among Teacher Trainees belonging to rural and urban areas.

Hypotheses: The following were the hypotheses of the study of the study

There is no significant difference in the cybercrime awareness among male and female Teacher Trainees

There is no significant difference in the cybercrime awareness among Teacher Trainees belonging to rural and urban areas.

Sample: The data was collected using a random sampling technique. A total of 200 B.Ed. students were chosen from Ludhiana's education colleges. There were 50 males and 150 females; and 100 rural and 100 urban among the 200 B.Ed. students.

Tool: The researcher developed his own cybercrime awareness scale. There are 42 sentences on this scale, 24 of which are positive statements and 18 of which are negative statements. Scores on the scale range from 42 to 210, with 42 suggesting very low awareness of cybercrime and 210 indicating very high awareness.

Analysis: Objective wise data analysis is as under:

The first objective was, "To compare the cybercrime awareness among male and female Teacher Trainees". The t-test was used to evaluate the data relevant to this goal. Table 1 summarises the findings:

Table 1 Significance of the Difference between Mean Scores of Cyber Crime Awareness of Male and Female Teacher Trainees

S.No.	Group	N	M	S.D	SEM	t-value
1.	Female Teacher Trainees	150	69.17	9.25	1.05	8.751*
2.	Male Teacher Trainees	50	87.46	8.01	1.00	

*significant at 0.01 level

Table 1 revealed that the mean scores of cybercrime awareness of female and male Teacher Trainees as 69.17 and 87.46 respectively and their standard deviation as 9.25 and 8.01 respectively. The t-value is 8.75 with df=198 which is significant at 0.01 level of confidence. This revealed that a significant difference exists between mean scores of cyber crime awareness of male and female Teacher Trainees. Therefore the first hypothesis namely 'there is no significant difference in the mean scores of cyber crime awareness of male and female Teacher Trainees' is rejected. Further as the mean scores of male Teacher Trainees (87.46) is higher than that of female Teacher Trainees (69.17), therefore, it may be said that male Teacher Trainees have significantly higher cyber crime awareness than their female counterparts.

The second objective was, "To compare the cybercrime awareness among Teacher Trainees belonging to rural and urban areas". The t-test was used to evaluate the data relevant to this goal. Table 2 summarises the findings:

Table 2: Significance of the Difference between Mean Scores of Cyber crime awareness of Rural and Urban Teacher Trainees

S.No.	Group	N	M	S.D	SEM	t-value
1.	Rural Teacher Trainees	100	60.30	8.67	1.16	13.76*
2.	Urban Teacher Trainees	100	96.32	13.17	0.91	

*significant at 0.01 level

Table 2 revealed that the mean scores of cyber crime awareness of rural and urban Teacher Trainees as 60.30 and 96.32 respectively and their standard deviation as 8.67 and 13.17 respectively. The t-value is 13.76 with df=198 which is significant at 0.01 level of confidence. This revealed that a significant difference exists between mean scores of cyber crime awareness of rural and urban Teacher Trainees. Therefore the hypothesis 2 namely ‘there is no significant difference in the mean scores of cyber crime awareness of rural and urban Teacher Trainees is rejected. As the mean score of urban Teacher Trainees (96.32) is higher than that of rural Teacher Trainees (60.30), therefore, it may be said that urban Teacher Trainees have significantly higher cyber crime awareness than their rural counterparts. Null hypothesis 2 was thus rejected.

Findings:

- 1) Male Teacher Trainees have significantly higher cyber crime awareness than their female counterparts
- 2) Urban Teacher Trainees have significantly higher cyber crime awareness than their rural counterparts

Implications: The study found that male Teacher Trainees are more aware than female Teacher Trainees, and urban Teacher Trainees are more aware than rural Teacher Trainees, indicating that female Teacher Trainees and Rural Teacher Trainees need special attention. As teachers shape our youth's future, it is proposed that government and institutions educate Teacher Trainees about cybercrime.

REFERENCES

[1]. Bhushan K. (2012), India ranks fifth among cybercrime affected country, retrieved from <http://www.thinkdigit.com>

[2]. International Telecommunication Union. (2012). Measuring the Information Society, and World Telecommunication/ICT Indicators Database.

[3]. Kumar, V.D. (2013). Cyber crime prevention and role of libraries. International Journal of Information Dissemination and Technology, 3(3), 222-224.

[4]. Mehta,S. &Singh,V.(2013).A study of awareness about cyber laws in the Indian Society. International Journal of Computing and Business Research (IJCBR),4(1).

[5]. Nappinai, N.S. (2010), Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study, N. S. Journal of International Commercial Law and Technology, 5(1), 22-28. Retrieved from <https://media.neliti.com/media/publication>

[6]. Shubhangi Taneja; Ruchi Pal; Shiwangi Vishwakarma; Rakesh Kumar. "A Case Study on Cyber bullying". International Research Journal on Advanced Science Hub, 2, 7, 2020, 29-31. doi: 10.47392/irjash.2020.60

[7]. Pandey K. (2012).Low security makes netizens vulnerable to cybercrimes. Retrieved from http://articles.timesofindia.indiatimes.com/indore/31863717_1_cyber-crimes-cyber-cellcyber-criminals on May 26, 2014.

[8]. Saxena P., Kotiyal, B. &Goudar, R.H. (2012), A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India. IACSIT International Journal of Information and Education Technology, 2(2).

[9]. Seth K. (2007), India – Cyber crimes and the arm of Law – An Indian Perspective, retrieved from <http://www.sethassociates.com>

[10]. Praveen Kumar Mishra; Prabhakar Tiwari. "Cyber Security in Smart Grid". International Research Journal on Advanced Science Hub, 2, 6, 2020, 26-30. doi: 10.47392/irjash.2020.33

[11]. Singaravelu,S. &Pillai,S.K.P. (2014).B.Ed.students awareness on Cybercrime in Perambalur District, International Journal of Teacher Educational Research (IJTER), 3(3).