ISSN 2278-8808
UGC APPROVED SR. NO. 45269
SJIF 2016 = 6.177
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

CYBER CRIME AWARENESS AMONG TEACHER TRAINEES

Taruna Malhotra[1], Ph. D. & Ms. Mona Malhotra[2]

Abstract

The purpose of the present investigation was to assess the level of cyber crime awareness among teacher trainees and to study the influence of gender, locality and their various interactions on the level of cyber crime awareness among teacher trainees. The sample comprised 240 teacher trainees selected randomly from six teacher trainee colleges (three from urban and three from rural areas) approved by NCTE, were selected randomly from Haryana. Data were analysed by adopting the criterion Mean ± SD and using two way ANOVA (2x2 factorial designs) and t-test. Results indicated that(i) most of the prospective teachers have comparatively moderate awareness level of cybercrime; (ii) there is significant independent effect of variables viz. gender and locality on the level of cyber crime awareness among teacher trainees; and (iii) there is significant two factor interactive effect of variables on the level of cyber crime awareness among teacher trainees.

Keywords: *cyber crime awareness and teacher trainees*

Introduction

In present scenario, information and communication technologies are omnipresent and digitalization in all areas is expanding and the world of internet today has become a parallel form of life and living.The usage of Internet is one of the fastest-growing areas of technical infrastructure development (Miao Y., 2007).The availability of ICTs is a foundation for development in the creation, availability and use of network-based services.The introduction of ICTs into many aspects of everyday life has led to the development of the modern concept of the information society as it offers great opportunities. Unhindered access to information can support democracy, as the flow of information is taken out of the control of state authorities, online banking and shopping, the use of mobile data services and voice over Internet protocol telephony are just some examples of how far the integration of ICTs into our daily lives and education system.E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials and Internet-based communication and phone services are growing faster than landline communications(Zittrain,2006).

But on the other side, the growth of the information society is accompanied by new and serious threats too, like different forms crime committed or facilitated via the Internet, may be termed as cybercrime. It can be said that cybercrimes are those crimes which have the involvement of computer and network (Fafinski, 2008). Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It as an intended act involving the use of computers or other technologies, and the criminal activity must take place in a virtual setting, such as the Internet (Florida Cyber-Security Manual, 2004).According to Council of Europe "Any criminal offence committed against or with the help of a computer network is identified as cybercrime" (Council of Europe Convention on Cybercrime 2001:8). So computer is must for cybercrime.It has some different name such as computer crime", "computer-related crime", "high-tech crime", "Internet crime"(Brenner and Goodman 2002, Kowalski 2002).

Cybercrimes share three elements:

1. Tools and techniques to perpetrate a crime

2. Approach or methodology for executing the criminal plan — known as a vector

3. Crime itself that is the end result of those plans and activities (a cybercrime is the ultimate objective of the criminal's activities).

Common Types of Cybercrime

Cybercrime	Description
Computer virus	A computer virus is a computer program that piggybacks or attaches itself to application programs or other executable system software; the virus subsequently activates, sometimes causing severe damage to computer systems or files.
Phishing	Phishing occurs when the perpetrator sends fictitious emails to individuals with links to fraudulent websites that appear official and thereby cause the victim to release personal information to the perpetrator.
Botnet	A Botnet infection occurs when a hacker transmits instructions to other computers for the purpose of controlling them, and then using them for various purposes such as spam or phishing.
Spoofing	Spoofing is use of email to trick an individual into providing personal information that is later used for unauthorized purposes.
E- theft	E- theft occurs when a perpetrator hacks into a financial institution e.g. a bank and diverts funds to accounts accessible to the criminal. To prevent e-theft, most major banks severely limit what clients can do online.
Netspionage	Netspionage occurs when perpetrators hack into online systems or individual PCs to obtain confidential information for the purpose of selling it to other parties (criminals).

Online credit card fraud	Online credit card fraud is illegal online acquisition of a credit card number and use of it for unauthorized purposes such as fraudulent purchases.
Online denial of service	Online denial of service is use of email barrages, computer viruses, or other techniques to damage or shut down online computer systems, resulting in loss of business.
Software piracy	Software piracy is the theft of intellectual assets associated with computer programs.
Spam	Spam refers to unsolicited email; spam is illegal if it violates the Can-Spam Act of 2003, such as by not giving recipients an opt-out method.
E-fraud	E-fraud is the use of online techniques by a perpetrator to commit fraud. Popular forms of e-fraud include spoofing, phishing, and online credit card fraud.
Cyber terrorism	Cyber terrorism occurs when terrorists cause virtual destruction in online computer systems

Review of related literature:

Higgins (2010) observes the use of computers and the change in technology due to new advancements. He also cautions the security of internet users and relates this to emergence of cyber crime. In one of his earliest studies conducted on the use of the Internet evaluates socio-psychological effect of Internet. It was noted that the more use of Internet is associated with a decline in communication among family members, decline in social association and increase in aggression and depression. Heuven and Botterman(2003) opine that e-frauds and identity thefts have caused financial loss on a global level and is a challenge for the nation's infrastructure and security, Kraut (1998). Brenner (2010) highlights the fact that common man has a limited knowledge about the crimes which occur in cyberspace. Knowledge is very important for everyone to prevent cybercrime (Wang et al., 2008). Chawki (2005) states that educating young people would help decrease the risk of students in cyberspace. Asokhia (2010) finds that the level of education contributes significant differences to the students' perceptions of cybercrime. Knowledge helps people to be more aware on cybercrime (Levin et al., 2008). Li, (2006) stated that there are dissimilar perceptions and awareness between men and women. According to Titi (2003) women are more aware of cyber regulations and have superior ethical values compared to men. Women are less likely to become victims as compared to men. Lifestyle Theory states that sex is an often-mentioned demographic characteristic that is associated with difference in lifestyle (Ngo and Paternoster, 2011). Based on the review of above literatures it is anticipated that gender and locality too have significant influences on cybercrime.

Rationale of the study:

The internet, as we know has grown rapidly over the last decade in India. It has given rise to many avenues in every field like education, entertainment, business or sports. However, every coin has two sides in the same manner; digitalization process has both pros and cons. The internet along with benefits has also exposed to security risks. Computers, today are being misused for unlawful activities like e-mail espionage, credit card fraud, spam, software piracy, spreading of viruses and so on, which invade our privacy and offend our senses. Criminal activities associated with computers and internets are globally rising. In fact, cybercrimes have risen so dramatically in recent years that they have seemingly replaced old-fashioned, organized crimes (Consumer Report, 2011). Basically, Cybercrime is any criminal activity involving computers and networks, which can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime incorporates anything from downloading illegal music files to stealing millions of rupees from online bank accounts. Generally Among the numerous crimes in today's society; cybercrime has become very common as well as very dangerous. The emergence of new technology has increased the number of perpetrators that take advantage of these resources to use them illegally for their own gain (Gjata 2007). Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day.

The proliferation of technology devices and other equipment; their pervasive use across age, gender, socioeconomic and geographic boundaries; and, for many, a false sense of information security have merged to create a perfect storm for cybercriminal activity. Also in teaching and learning, the use of computers and internet is inevitable and of course one should update him or herself regarding risk factors attached to it. Hence the awareness of cybercrime is very much needed for the learners and also for the teachers. There is dearth of studies which try to study the level of cybercrime awareness among teacher trainees. So, the present investigators visualized a need to study level of cybercrime awareness among teacher trainees and this paper elucidates the awareness of teacher trainees towards cybercrime.

Operational Definition of the Terms

Teacher Trainees: The students studying in Colleges of Education enrolled under M. D. U. and C. R.S. U. during the session 2016-2017.

Cybercrime: "Any criminal offence committed against or with the help of a computer network is identified as cybercrime" (Council of Europe Convention on Cybercrime 2001).

Objectives

1. To study the level of cybercrime awareness among teacher trainees.

2. To study the influence of gender, locality and their various interactions on cybercrime awareness of teacher trainees.

Hypothesis

There is no significant influence of gender, locality and their various interactions on cybercrime awareness of senior secondary school students.

Tools Used

Following tests were used to obtain reliable data:

1. ***Cyber Crime Awareness Scale (CCAS) by Rajasekar(2011):*** CCAS intends to measure the awareness on cybercrime of B. Ed. Students. The scale consisted of 42 statements, out of which 24 were positive statements and the remaining 18 were negative statements. Each statement was against five point scale from strongly agree, agree, undecided, disagree to strongly disagree and weightage of 5, 4, 3, 2, 1 were given in the order for positive statements and scoring is reversed for the negative statements. The construct validity of the scale was found to be 0.87 and reliability was determined by using the Spearman-Brown prophecy formula, was found to be 0.76.
2. ***Personal Information Schedule (PIS)*** developed by investigator to get the information like gender and locality.

Sample and Procedure

For collecting data, six teacher trainee colleges (three in urban and rural areas) approved by NCTE, were selected randomly from Haryana. The investigator personally visited the Colleges of Education one by one. After rapport formation she administered the tools to prospective teachers present on the day. After collecting the tools back, those cases were discarded who didn’t have even basic knowledge of computers or who did not belong to moderate level of intelligence; as review suggested that students who own computer has more computer knowledge than those who do not (Al-Badar,1993) and IQ has significant relationships to students’ achievement regarding knowledge of computers (Tipton, 1991). Then on the basis of Mean and S.D., the teacher trainees were divided into four parallel groups —males studying in urban locality, males studying in rural locality, females studying in urban locality and females studying in rural locality. From each of these groups, 60 teacher trainees were selected randomly, that is 60 from each combination group. In this way final sample comprised 240 prospective teachers as given inTable1

Distribution of Sample

Table 1

Gender (A)	Locality (B)	N
Males (A1)	Urban (B1)	60
	Rural (B2)	60
	Total	120
Females (A2)	Urban (B1)	60
	Rural (B2)	60
	Total	120
Total	Urban	120
	Rural	120
	Total	240

Statistical Techniques Employed

To find out the level of cybercrime awareness among teacher trainees, criterion of Mean ± SD was applied to scores of cybercrime awareness scale. In order to study the influence of gender and locality towards cybercrime awareness and their various interactions on cybercrime awareness twoway ANOVA (2×2 factorial design) was employed. The first independent variable gender (A) varied in two ways — Males (A1) and Females (A2); and the second independent variable locality (B) varied in two ways — Urban (B1) and rural (B2). In case of significant main effects as well as interactions, the ANOVA was supplemented by *t*-test.

Analysis and Interpretation

In pursuance of the objectives data were analyzed and interpreted under the following heads:

1. **Level of cybercrime awareness among teacher trainees:**

   In the present investigation, 240 subjects were classified into six groups by adopting the criterion of Mean ± SD to their score exam anxiety level as follows:

Table 2 Classification of Subjects into Six Groups on the Basis of their Score in Cyber Crime Awareness Scale

Sr. No	Level of Cyber Crime Awareness	Range of Scores	N (%)
1	Excellent Awareness	143 or above	8(3%)
2	High Awareness	133-142	22(10%)
3	Above Average Awareness	132-122	42(17%)
4	Moderate/Average Awareness	108-122	148(62%)
5	Below Average Awareness	99-107	14(5%)
6	Low Awareness	88-98	6(2%)

Results in Table 2 reveal that majority of teacher trainees had moderate or average (62%) followed by above average (17%), high (10%) and excellent awareness (3%). A small percentage of subjects (5%) and (2%) fell in the category of below average and low awareness.

2. **Influence of gender, Locality and their various interactions on Cybercrime awareness among teacher trainees:**

The summary of Two Way ANOVA (2×2) is given in Table 3

Table 3 Summary of 2×2 Two Way ANOVA of Level of Cyber Crime Awareness

Source of Variance	Df	Sum of squares	Mean Squares	F-value	Remark
A	dfA= 1	SSA = 3345.06	MSA=3345.06	FA =24.96	P<.01
B	dfB= 1	SSB= 2306.4	MSB= 2306.4	FB = 17.21	P<.01
A×B	dfA× B=1	SSA×B= 3776.27	MSA×B=3776.27	FA×B=28.18	P<.01
Within SS	dfW= 236	SS W =31622.667	MS W =133.994		
Total	239	41050			

2.1.Cyber Crime Awareness by Gender

From Table 3 it can be seen that the F-value for gender is 24.96, which is significant at 0.01 with df = 1/256. It shows that gender significantly influenced the level of cybercrime awareness among teacher trainees. Thus the null hypothesis that there is no significant influence of gender on level of cybercrime awareness among teacher trainees is rejected. In order to interpret this, t-test was applied. The results for the same have been given in Table 4.

Table-4 Gender Wise Mean, SD and *t*-value of Level of Cybercrime awareness

Gender (A)	N	Mean	SD	t-value	Remark
Males (A1)	120	105.33	12.15	4.47	P<.01
Females (A2)	120	98.06	13		

2. 2.**Cyber Crime Awareness by Locality**

The F-value for locality wise level of cybercrime awareness of prospective teachers is 17.21 (vide Table 3), which is significant at 0.01 level. It may, therefore, be said that locality towards cybercrime awareness significantly influenced the teacher trainees. Thus, the null hypothesis that there is no significant influence of locality on the level of cybercrime awareness among teacher trainees is rejected. In order to interpret this, *t*-test was applied. The results have been given in Table 5.

Table 5 Locality Wise Mean, SD and t-value of level of Cybercrime awareness

Locality (B)	N	Mean	SD	t-value	Remark
Urban (B1)	120	104.90	12.27	4.15	P<.01
Rural (B2)	120	98.70	13.22		

From Table 5 it is evident that *t*-value is 4.15, which is significant at 0.01 level of significance. It indicates that the mean scores of locality among teacher trainees belonging to urban and rural locality differ significantly. Thus, the null hypothesis that there is no significant difference in mean scores of locality among teacher trainees belonging to urban and rural locality is rejected. Further, mean scores of locality among teacher trainees belonging to urban locality is 104.90, which is significantly higher than that of belonging to rural locality whose mean score of cybercrime awareness is 98.70. It may, therefore, be said that cybercrime awareness was found to be significantly more in case of urban teacher trainees in comparison to teacher trainees belonging to rural locality.

2.3. **Two Factor Interaction Effect on Level of Cyber Crime Awareness**

2.3.1 **A x B Interaction**

The F-value for the double interaction between Gender and Locality (A x B) is 28.18 (vide Table 3 for df= 1/236) is significant at 0.01 level, leading to inference that the two variables interact with each other. To investigate further, the interaction between gender and locality, the t-ratios were computed. The results for the same have been given in Table 6

Table 6 Significance of Difference of Mean scores of level of Cyber Crime Awareness among Different Combination Groups for Gender x Locality

Group (Mean)	A1B1(106.4))	A1B2(104.6)	A2B1(105.13)	A2B2(91)
A1B1 (106.4)	-	0.78	0.21	5.93**
A1B2 (104.66)	-	-	0.67	7.83**
A2B1 (105.13)	-	-	-	7.17*
A2B2 (91)	-	-	-	-

Table 6 shows that male teacher trainees belonging to urban locality have more cybercrime awareness (M=106.4) than females teacher trainees belonging to urban locality (M=105.13). Male teacher trainees belonging to urban locality are having more cybercrime awareness

(M=106.4) as compared to female teacher trainees belonging to rural locality (M=104.6). Maleteacher trainees belonging to urban locality (M=106.4) as compared to females teacher trainees belonging to rural locality (M=91)yield comparable mean scoreson cybercrime awareness. Female teacher trainees belonging to urban locality (M=105.13) are more aware about cybercrimes than males teacher trainees belonging to rural locality (M=104.6). Female teacher trainees belonging to urban area have more awareness regarding cybercrimes (M=105.13) than female teacher trainees belonging to rural locality (M=91). Male teacher trainees belonging to rural locality yield comparable mean scores on cybercrime awareness (M=104.6) as compared to female teacher trainees school belonging to rural locality (M=91). Further, male teacher trainees mean scores on cybercrime awareness belonging to urban locality have maximum cybercrime awareness (M=106.4), while males teacher trainees belonging to rural locality have lowest level cybercrime awareness (M=91).

Findings

1. There is significant difference in the level of cybercrime awareness among teacher trainees with respect to gender.
2. There is significant difference in the level of cybercrime awareness among teacher trainees with respect to locality.
3. There is significant difference in the level of cybercrime awareness among teacher trainees with respect to gender and locality.

Discussion

Results of the present study indicate that only 10 per cent of the teacher trainees have excellent cybercrime awareness. 17 per cent of them are above average, 62% have average cybercrime awareness, 5% have below average awareness whereas 2 % have low awareness regarding cybercrimes. It means that teacher trainees understand that to excel in present competitive world one must have updated knowledge and should be techno-savvy and to achieve in a better way; one must have familiarity of digitalized world. But some teacher trainees develop fear for such situations and become over cautious whereas few are irresponsible and develop careless attitude by having low level of awareness. Cybercrime is a new wave of crimes using internet facilities, which needs to be addressed urgently and earnestly by policy planners to protect theyoung generation as there is a high risk of becoming avictim of this crime (Mensch and Wilkie,2011). Human beings are usually the first line of defense to secure information assets, no matter how advanced and rigid the security technology solutions may be. All the security breaches such as virus infections, identity theft and hacking are the direct cause of carelessness and lack of knowledge and action on the part of users (Chen et al., 2008).

Welsh (2011) calls today's generation as "digital natives" or the "i-Generation". Today's highly complex, inter connected, global information systems provide an extensive attack surface that is almost impossible to secure. Regulatory measures such as legislation, court action and even industry wide security standards often fail to keep pace with rapid changes in technology. Countering misuse and abuse in such an environment is a constant battle. Oates (2001) stresses the importance of preventing, detecting, investigating, and prosecuting cybercrimes with the goal of reducing their impact on business and the public's confidence. In order to stop cybercrime, the private, public, and international sectors must openly share information on the methods they are successfully using to detect and prevent these crimes.

A high level awareness about information security and cybercrime issues amongst users at home, in government and educational institutions, especially young people, would decrease the occurrence of cybercrime (Sembok, 2003). The effectiveness of combating cybercrime among users' especially would be teachers will work if they are familiar and adroit while using online. Therefore, human factors such as gender, locality may assist in augmenting the levels of awareness among new generations. In this way, Students' perceptions of risk and awareness on security of the internet and information should be profoundly addressed (Wang et al., 2008). The number of cybercrime victims could be reduced by introducing proper awareness activities such as training programs, sufficient resource for compliance, develop policies & regulations and sufficient protection of personal information (Bougaardt and Kyobe, 2011). Choi (2008) emphasizes on the effectiveness of university programs in promoting knowledge and values about cybercrime as these programs could improve future behaviour of students and teachers towards cybercrime in terms of safety and security.

References

Al-Badar, M. (1993), Predictors of success in self-instructional courses on microcomputer application software. (online) Dissertation Abstracts International, 5408A.2991. Abstract from: Ohio link file: Dissertation abstracts international item: AA19005361.

Asokhia, M., (2010), Enhancing national development and growth through combating cybercrime internet fraud: A comparative approach. J. Soc. Sci., 23: 13-19.

Bougaardt, G. and M. Kyobe, 2011. Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. Electr. J. Inform. Syst. Evaluat., 14: 167-178.

Brenner,W.S. (2010), Cybercrime:Criminal threats from cyberspace. Greenwood Publishing group, Westport.

Chawki, M., (2005), A critical look at the regulation of cybercrime. ICFAI J. Cyberlaw, 3: 1-55

Chen, C.C., B.D. Medlin and R.S. Shaw, 2008. A cross-cultural investigation of situational information security awareness programs. Inform. Manage. Comput. Security, 16: 360-376. DOI: 10.1108/09685220810908787

Choi, K., 2008. Structural equation modeling assesment of key causal factors in computer crime victimization. Ph.D Dissertation, Indiana University of Pennsylvania, USA.

Consumer Reports, June 2011 issue online, Available at: consumerreports.org.

Dashora K. (2011) Cyber Crime in the Society: Problems and Preventions, Journal of Alternative Perspectives in the Social Sciences , Vol. 3, No 1, 240-259

Fafinski, S. (2008). UK Cybercrime report Retrieved from http://www.garlik.com

Florida Cyber-Security Manual (Nov. 2004), Secure Florida, p. 150. Available at: secureflorida.org.

Gjata, O. (2007), Cybercrime. Retrieved from http://mason.gmu.edu/~ogjata/index.html

Heuven M. & Botterman S. (2003), Managing New Issues: Cyber Security in an Era of Technological Change [Kindle Edition] Rand

Higgins, George (2010), Cybercrime: An Introduction to an Emerging Phenomenon, McGraw Hill Publishing, New York.

Kowalski, M. (2002). Cyber-Crime:Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics. Catalogue No. 85-558-XIE, ISBN 0-660-33200-8. Retrieved from http://statcan.gc.ca/pub/85-558-x/85-558-x2002001-eng.pdf

Kraut, Robert and Patterson, M and Lundmark, V. and Kisler, S and Mukhopadhyay, T and Scherlis, W (1998), Internet Paradox – A Social Technology that reduces social Involvement and Psychological well being ? American Psychologist, Vol.53(9), 1017- 1031.

Levin, A., M. Foster, B. West, M.J. Nicholson and T. Hermandez et al., (2008), The next digital divide: Online social network privacy. Privacy and Cybercrime Institute, Ryerson University, Canada.

Li, X., 2006. The criminal phenomenon on the internet: Hallmarks of criminals and victims revisited through typical cases prosecuted. University Ottawa Technol. J., 5: 125-140.

Mensch, S. and L. Wilkie, 2011. Information security activities of college students: An exploratory study. Acad. Inform. Manage. Sci. J., 14: 91-116.

Miao Y. (2007), ACM International Conference Proceeding Series; Vol. 113, page 52 – 56; available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007

Ngo, F.T. and R. Paternoster, (2011), Cybercrime victimization: An examination of individual and situational level factors. Int. J. Cyber Criminal., 5: 773-793.

Oates, B. (2001). Cyber Crime: how technology makes it easy and what to do about it. Information Systems Security, 9(6), 1-6

Sembok, T.M., 2003. Ethics of information technology. Proceedings of the Regional Meeting on Ethics of Science and Technology, RUSHAP, UNESCO, Nov. 5-7, Bangkok.

Sharpening Europe's Future Through ICT (2006), Report from the information society technologies advisory group, 2006, available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/istagshaping-europe-future-ict-march-2006-en.pdf.

Tipton, M. (1991). The effect of ability, age, attitude and gender on students' achievement in the junior high computer literacy class. (online) Dissertation Abstracts International, 30-04A, 1016. Abstract from: Ohio link file: Dissertation abstracts international item : AA11347809.

Titi, K.M., (2003), Code of ethics, professionalism and responsibilities, Al-Ahliyyah Amman University, Ardhah, Jordan.

Wang, H.S., Chou C.H. and Tsai S.N. (2008), A preliminary study of the education of internet security implied in a movie based English class in Taiwan's private vocational continuation high school. CNTE2008, Chichu, Taiwan.

Welsh, Jennifer (2011). Is Constant 'Facebooking' Bad for Teens? Livescience, 6 Aug. 2011.

Zittrain (2006), History of Online Gatekeeping, Harvard Journal of Law & Technology, , Vol. 19, No. 2.