From Awareness to Action: A Cyber Security Agenda in Digital Age

Eisha Verma

Research Scholar, Department of Educational Studies, Central University of Jammu, Jammu and Kashmir, (India)

ABSTRACT

Cyber-crime is emerging as a very serious threat in today's world. It is the fast growing area of crime. As the internet users have increased considerably, so does the cyber-crime. The internet brings joy to our lives but at the same time it has some negative sides too. The cyber criminals are always in a search to find out the new ways to attack the possible internet victims. Today, everybody is using the computers i.e. from white collar employees to terrorists and from teenagers to adults. All the conventional crimes like forgery, extortion, kidnapping etc. are being done with the help of computers. Therefore, it has become very important for us to be aware of the cybercrimes. The present paper focuses on to provide a glimpse of various types of cybercrimes prevalent in modern technological society. This paper also attempt to find out the level of awareness about cyber-crime among students of Central University of Jammu. In addition, the investigator tried to see the differences in cyber-crime awareness among university students in relation to their gender, locality and stream. For the study descriptive survey design was used with sample of 250 students of different departments with the help of simple random sampling technique. The data for the study was collected by using cyber-crime awareness scale by Dr. S. Rajasekar and the collected data was analyzed with the help of critical ratio. The findings of the study revealed that there are significant gender differences in the cyber-crime awareness. Hence the results have important implications in order to increase student's level of awareness.

Key words: Awareness, Agenda, Cyber-crime, Digital, and Security.

I. 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 2007)** [(1)]**.**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)** [(2)]**.**

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)** [(3)]**.** Cybercrime is defined as crime 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)** [(4)]**.** 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,**[(5)] **Kowalski 2002)**[(6)]**.**

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).

I.1. CATEGORIES OF CYBER CRIME

Cyber-crime can be categorized as, the crime against:

A. Individual

Cyber-crimes which are done to harm a particular individual come under this category. The crime against individual can be such as cyber stalking, trafficking, grooming and distributing pornography.

B. Property

Cyber-crime which is done to harm the property of an individual or of any organization comes under this category. This type of crime involves stealing and robbing i.e. criminals can steal person's bank details and transfer money to his account; criminals can misuse the credit card details of the person to purchase online; criminals can use special software to steal organization's confidential data; malicious software can also damage the hardware and software of the organization.

C. Government

Crimes against government are known as cyber terrorism. Cyber-attacks against government are not as common as other two categories. Criminals attack government websites, military websites which create chaos among civilians.

I.2. TYPES OF CYBER CRIME

Cyber-crimes can be of the following types:

A. Hacking- It is a type of crime in which person's computer is accessed by criminals. Hacking is done to access the personal, confidential and sensitive information from an individual's computer. It can also be done to change the passwords of login accounts and use the information against them.

B. Theft- Under this category a person violates or breaks the copyrights of a particular website and download songs, games, movies and software. There are many websites which allow downloading the data that is copied from other websites. It is known as pirated data as the quality of data is not up to the mark.

C. Identity theft- In this attack, criminals steal data about person's bank account number, credit card number, debit card and other confidential data to transfer money to his account or buy things online by acting as the original person i.e. the criminal stalks the identity of person and thus it is known as identity theft. This theft can result in huge economical loss to the victim.

D. Defamation- In this type of crime, the criminal hacks the email account of a person and sends mails using abusive languages to known person's mail accounts so as to lower the dignity or fame of that person.

E. Malicious software- These are the software that is used to access the system to steal confidential data of the organization or can be used to damage the hardware and software of the system.

F. Cyber Stalking- It is a type of attack where online messages and e-mails are bombarded on victim's system. In cyber staking, internet is used to harass an individual, group or organization by using defamation, identity theft, solicitation for sex, false accusations etc.

G. E-mail harassment- In this type of cyber crime, the victim is harassed by receiving letters, attachments in files and folders of e-mails.

H. Spoofing- It is a type of situation in which criminal masquerade as another person i.e. the criminal acts as another person by using his identity and therefore takes advantage of illegally accessing data of the other person.

I. Virus- It is a small program that is loaded on the victim's computer without his knowledge which causes a large amount of damage to the system. Viruses attach themselves to files and circulate themselves to other files on the network which leads to damage of the system.

J. Phishing- It is an attack in which criminal sends genuine looking emails to victim to gather personal and financial information of the victim which can be used against him.

K. Grooming- Grooming is the process of influencing the children and youth emotionally for sexual exploitation. In this process, criminal wins the trust of victim by giving flattery offers and then attempts to sexualize the relation between them which leads to pornography or sex trafficking.

II. JUSTIFICATION OF THE STUDY

The internet, as we know has grown rapidly over the last decade in India. It has given rise to many directions 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 advantages has also manifested 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. 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)** [(7)]**.** Basically, cybercrime is any criminal activity involving computers and networks, which can range from fraud to unsolicited email spam. Among the various crimes prevailing 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)** [(8)]**.** Online fraud and hacking attacks are just some examples of computer-related crimes that are committed on a large scale every day. Hence the awareness of cybercrime as well as cyber security is very much needed for the learners and also for the teachers. There is dearth of such studies which try to study the level of cybercrime awareness. So, the present investigation visualized a need to study level of cybercrime awareness among students and this paper elucidates the awareness of students towards cybercrime.

III. OBJECTIVES OF THE STUDY

The following were the objectives of the study:

1. To study the gender differences in cyber-crime awareness among university students.
2. To study the differences in cyber-crime awareness among university students in relation to their locality.
3. To study the differences in cyber-crime awareness among university students in relation to their stream.

IV. HYPOTHESES OF THE STUDY

On the basis of the objectives of the study following hypotheses were drawn:

1. There will be no gender differences in cyber-crime awareness among university students.
2. There will be no differences in cyber-crime awareness among university students in relation to their locality.
3. There will be no differences in cyber-crime awareness among university students in relation to their stream.

V. DELIMITATIONS OF THE STUDY

The present study was confined to the following areas:

1. The study was delimited to the students of Central University of Jammu only.
2. The study was delimited to a sample of 250 students only.
3. The study was delimited to post graduate students only.

VI. POPULATION

In the present study all the students studying in the post graduate departments of Central University of Jammu constituted the population**.**

VII. SAMPLE

In the present study, the sample of 250 students studying in post graduate departments of Central University of Jammu was randomly selected.

VII. STUDY DESIGN

The investigator has adopted descriptive survey method for conducting the study.

IX. TOOL USED

In order to collect the requisite data the investigator used the cyber-crime awareness scale by S. Rajaseka.

X. STATISTICAL TECHNIQUES USED

For the analysis and interpretation of data the following techniques were used:

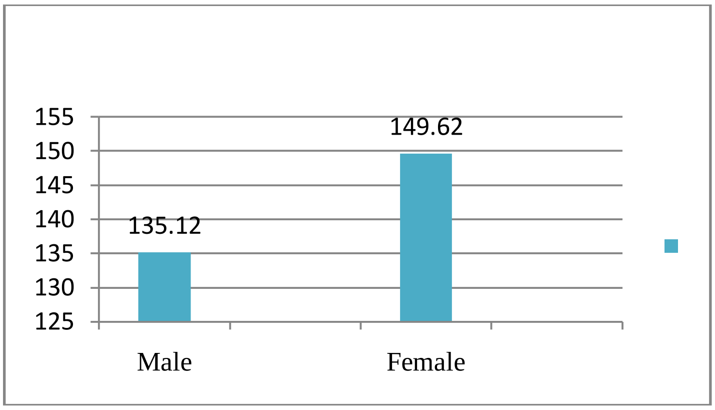
1. Mean
2. Standard deviation
3. Critical ratio

XI. RESULTS AND DISCUSSIONS

Table 1: critical ratio of mean score of university students towards cyber-crime in relation to their gender

Variables		N	M	σ	C.R.	Level of Significance
Gender	Male	123	135.12	15.83	6.85	Significant
	Female	127	149.62	17.60		

From the above table it is clearly evident that the critical ratio of mean score of male and female students towards cyber-crime awareness was significant. The table clearly shows that the critical ratio of mean score of male and female students was significant at .01 level of significance. As calculated value of C.R. (i.e.6.85) is greater than 2.58 which is table value at 0.01 level. Therefore it can be said that there are significant differences in the cyber-crime awareness of the male and female students.



Also by further comparing mean value we can say that the mean score of female students (M =149.62) is more than the male students (M=135.12) which means female students are more aware about the cyber crime than their male counterparts. Hence, the (Hypothesis H1) which states that there will be no gender differences in cyber-crime awareness among university students was rejected.

Table 2: critical ratio of mean score of university students towards cyber-crime in relation to their locality

Variables		N	M	σ	C.R.	Level of Significance
Locality	Rural	100	142.72	18.49	0.57	Not Significant
	Urban	150	140.07	16.47		

The above table clearly reflects that the critical ratio of mean score of the subjects in their cyber-crime awareness on the basis of their locality was not significant. Therefore it can be said that rural and urban area students do not differ significantly in their cyber-crime awareness.

Hence, the (Hypothesis H2) which states that Therefore it can be said that there are significant differences in the cyber-crime awareness of the male and female students.

Table 3: critical ratio of mean score of university students towards cyber-crime in relation to their stream

Variables		N	M	σ	C.R.	Level of Significance
Stream	Humanities	115	140.62	18.39	0.38	Not Significant
	Science	135	141.54	19.07		

It is evident from the above table that the critical ratio of mean score of the subjects in their cyber-crime awareness on the basis of their stream was not significant. Therefore it can be said that the students belonging from humanities and science stream do not differ significantly in their cyber-crime awareness.

Hence, the (Hypothesis H3) which states that there will be no differences in cyber-crime awareness among university students in relation to their stream was accepted.

XII. RECOMMENDATIONS

It has been rightly said that prevention is always better than cure so it is always better to take certain precautions while operating the internet. So one should keep in mind the following:

1. One should not give their identifying information such as their name, home address, school name, phone number in chat room. They should also be advised not to give their photographs to anyone, not to respond to the messages which are obscene, threatening or suggestive. They should remember that people online might not be who they seem.
2. Parents should use content filtering software on their computers so that their child is protected from the pornography. Software can also be installed to establish time records i.e. blocking usage after particular time. Parents should also visit the sites visited by their children.
3. Keep back-up volumes so that one may not suffer data loss in case of virus contamination.
4. One should always use latest and update anti-virus software to protect their computer against virus attacks.
5. Never send your credit card number to any one or any site which is not secured.
6. Do not panic if you find something harmful. If you feel any danger, contact your local police. Moreover avoid getting into huge arguments online during chat and discussions.
7. Be cautious on meeting online introduced person. If you choose to meet, do so in a public place along with a friend. Try to keep record of all your communication for evidence. Do not edit it any way.
8. The use of password is most common for security of the system. Mostly all the systems are programmed to ask for username and password to access the computer system. Password should be changed after regular interval of time and should be difficult to judge.

CONCLUSION

With the increase in the users of internet, the increase in cyber-crimes can also be seen. Cyber-crime can be done mainly by using the technique of hacking. Hacking is the method in which the criminals get access to the victim’s system without their knowledge. All the persons who use internet and especially those make money transactions through internet must be beware of the cyber criminals. It is the need of today’s world to have knowledge about the crimes that are associated with the internet. It is the duty of each one of us to be aware of the basic internet security like changing the passwords regularly, keeping long passwords, avoids disclosing personal information to strangers on the internet or entering credit card details on unsecured websites to avoid any fraud, etc. Government is also making efforts to have a control on these cyber-crimes. Government has made cyber laws in order to help people learn about the cyber-crimes and cyber security. IT Act 2000 is made to deal with the cyber-crimes. Both the government and people should work hand in hand to catch the criminals. People who have been the victim of cyber-crime should come forward and file a complaint against the crime in special anti-cybercrime cells. Government should also employee officers with very high intelligent quotient and the knowledge about all the cyber-crimes. This will help to catch the criminals very easily and all the criminals must be given hard punishments which can a lesson for millions of other cyber criminals.

REFERENCES

[1] Miao Y. (2007), ACM International Conference Proceeding Series; Vol. 113, page 52 – 56; available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007.
[2] Zittrain (2006), History of Online Gatekeeping. Harvard Journal of Law & Technology, 19(2).
[3] Fafinski, S. (2008). UK Cybercrime report Retrieved from http://www.garlik.com.
[4] Florida Cyber-Security Manual (Nov. 2004), Secure Florida, p. 150. Available at: secureflorida.org.
[5] Brenner, S. W., & Goodman, M. D. (2002). In defense of cyberterrorism: An argument for anticipating cyber-attacks. U. Ill. JL Tech. & Pol'y, 1.
[6] 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
[7] Consumer Reports, June 2011 issue online, Available at: consumerreports.org.
[8] Gjata, O. (2007). Cybercrime. Retrieved from http://mason.gmu.edu/~ogjata/index.html.