

## **COMBATING THE CYBERCRIME: PRACTICES IN INDIAN SOCIETY**

Saroj Mehta & Vikram Singh

Department of Computer Science.

Ch Devi Lal University, Sirsa( INDIA)

**Abstract-** Information technology plays an important role in the management of air traffic control, nuclear power plants, electric power grid and communication of various institutions to specific purpose. Many companies rely on computer for managing payments, sales, production and inventories by the way of internet, telecommunication, online computing, etc. IT also plays an important role in prevention, detection, and mitigation of terrorist activities. It provides identification of patterns of behavior. The information revolution has brought both positive and negative changes to businesses, job markets, international affairs and every day life. Trends in information technology development are affecting both criminal activities and crime prevention. Information technology has facilitated individuals involved in criminal activities with reduced chances of detection. In this paper various trends for combating cybercrime among internet users have been studied and reported.

**Keywords –** Cybercrime, e-mail spoofing, e-mail bombing, technoculture, netizen.

### **I. Introduction**

Cybercrime is the involvement of individuals and/or group in criminal activities in which computer or computer network are tool, target, or place of criminal activities. It includes everything from electronic cracking to denial of service attacks to cyber stalking to spamming. It is also used in traditional crimes in which computers or networks are used to enable the unlawful activities. In cybercrime, the “cyber” component usually refers to perpetrating qualitatively new offences enabled by information technology or it refers to integrating cyberspace into traditional criminal activities. A generalized definition of cybercrime may be: “unlawful acts wherein the computer is either a tool or target or both”. The computer may be used as a tool in the following kinds of activity- financial crimes, sale of

illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target of unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

According to Casey (2000) cybercrime as “a crime related to technology, computers, and the Internet” and place cybercrimes within several distinct categories; cracking, piracy, phacking, cyber-stalking, cyber- pornography and cyber terrorism. Toyne (2003) defines cybercrime as “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.

In topical crime scenario it is well said that “the computers are the most dangerous tool to commit untraceable and virtual crime”. Unfortunately, the power of computing may fall in the hands of those who are having the best knowledge in computing and they are well known that the law is still unwritten in many of the cyber crime scenes. Here comes the role of the netizens to combat cyber crime/criminals using the techniques and the need of study regarding different between the gender combating cybercrime(s). The rates of the cybercrime are skyrocketing as per various studies conducted for the loss due to cybercrime.

## **II. REVIEW OF LITERATURE**

CCRC (2005) suggests that a broad, inclusive focus is necessary to address problems of cybercrime, going beyond criminal law, penal procedures and law enforcement. The focus should include requirements for the secure functioning of a cyber-economy optimizing business confidence and individual privacy, as well as strategies to promote and protect the innovation and wealth-creating potential and opportunities of information and computing technologies, including early warning and response mechanisms in case of cyber attacks..

In Geetha B (2011), the author has reported that the cybercrimes have grown in numbers and character. Women, the chosen victims of cybercrimes choose to remain silent about them due to outdated stereotypes — which complicates implementation of the IT Act. .

Untila A (2012) has discussed the worldwide nature of cybercrime by observing that “the task of combating cybercrime cannot be taken on by one country or region alone. It is an issue that can be resolved only through the combined efforts of members of the international community”.

Munyua A, et al. (n.d.) have emphasized the role of education and empowerment as a key component in addressing the problem of cybercrime. They have stated that “If individuals are given clear direction about how to protect themselves against threatening or harassing communications, and how to report incidents when they do occur, both industry and law enforcement will be in a position to cooperate to conduct investigations.” Both, Clark (2004) and Yar (2005) have placed cybercrimes within three categories, namely, software piracy, electronic break-ins, and computer sabotage.

### III. RESEARCH DESIGN

The investigator herself has prepared and standardized the test which measure responses on a five point Likert scale. The study aimed to collect responses with regards to the knowledge and awareness of respondents towards combating cybercrime while using the internet for various purposes. Such data were collected from the undergraduate and postgraduate students, teachers, and employee in IT sector belonging to Sirsa, Faridabad and Gurgaon districts of Haryana. The selection has been made so, so as to provide a geographical balance to the study.

An individual participant constituted the sampling unit whereas probability sampling (random sampling) techniques were used to select the sample of 400 respondents from a large finite population which was characterized by a Gaussian or normal sampling distribution. Table 1 shows the break-up of the sample:

Table 1 Break-up of sample

| Gender<br>Category      | Male | Female | Total |
|-------------------------|------|--------|-------|
| <b>Students/Teacher</b> | 150  | 100    | 250   |
| <b>Employee</b>         | 80   | 70     | 150   |
| <b>Total</b>            | 230  | 170    | 400   |

Test items were written to cover the entire content and the research objective. Care was taken that no objective remained untested. The test was got scrutinized. The test so prepared was given to the students/teachers/ employees and arranged in descending order subjected to Kelley's items analysis techniques as per their achievement scores, upper 27% which formed the upper group and the lower that formed the lower group were taken up for computing the internal

consistency discrimination index and the difficulty value of the test. For this, the number of correct responses to an item in each of the two groups was identified and tabulated. The formula for calculating difficulty value DV and discriminating power DP of each item is:-

$$Dv = \frac{Ru + Rl}{N} \qquad Dp = \frac{Ru - Rl}{0.5 N}$$

Where Dv = Difficulty value of the items      Dp= Discriminating power of the items.

Ru= Number of right responses in the upper group

Rl= Number of right responses in the lower group

N= Total number of students in both group

For the selection of items the criteria recommended by 'Ebel' were given due consideration. Table 2 shows the criteria for selecting items on the basic of discriminating power (Dp).

Table 2: Selection criteria of items

| Sr. No | Discriminating Power | Item Evaluation                               |
|--------|----------------------|---|
| 1      | 0.40 and above       | Very Good                                     |
| 2      | 0.20 to 0.39         | Marginal items usually subject to improvement |
| 3      | Below 0.19           | Poor items                                    |

After calculating the discriminating power of the items, criteria given in table 2 was applied to select the items for the final test items. The variables were categorized as independent and dependent variable. The dependent variables for the present study were the techniques for combating cybercrimes. Independent variables for the present study were employee/teacher and student having UG/PG education in the field of information technology / computer science and were using IT by means of internet, networking etc.

#### IV. RESULTS AND DISCUSSIONS

In the present study the aim was to study and compare the opinions of different subgroups in target sample with regards to combating cybercrime. CR ratio is useful for testing the significance of means separately for each part of the group. So the t- test was used to analyze the data and to find out the

significance of difference between two groups taken at a time. The data was analyzed with the help of Mean, SD, SE, CR ratio to find out the differences of the groups.

$H_{01}$ :- There is no significant difference in opinions of male employees and male students / teachers for the techniques combating cybercrime.

Table 3: Mean, SD, DF and CR ratio

| .Variables               | N   | Means | SD.   | DF. | CR.  | Level of Significance                            |
|--------------------------|-----|-------|-------|-----|------|--|
| Male Employees           | 80  | 85.32 | 16.87 | 228 | 4.98 | Significant at .05 and .01 level of significance |
| Male Students / Teachers | 150 | 73.25 | 18.76 |     |      |  |

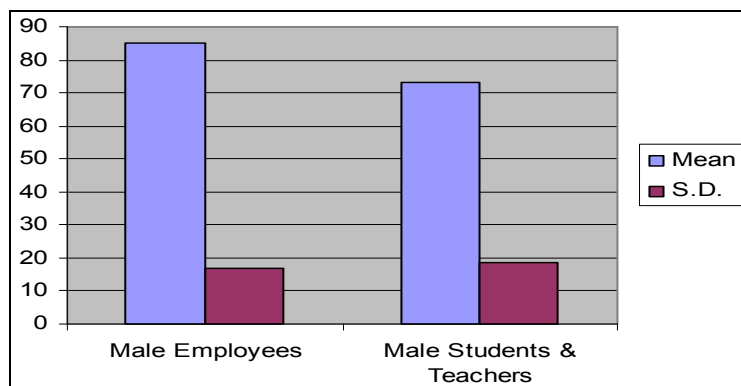


Figure 1: cybercrime combating techniques (male)

Table 3 indicates that the mean scores of the opinions of male employees in combating cybercrime is 85.32 and the mean score of male students/teachers in combating cybercrime is 73.25 and their SD values are 16.87 and 18.76 respectively. The CR value comes out to be 4.98 which is significant at .05 and .01 level of significance at DF value = 228. This further reveals that the two groups differ significantly because the table value at DF =228 are 1.97 at .05 level of significant and 2.60 at 0.01 level of significance are lower than the calculated value; see figure 1. It is concluded that male employees and male students/teachers differ significantly and the mean value of male employee is greater than male students/teachers. Therefore it is analyzed that the more male employees are interested in combating cybercrime than male student/teachers. The corresponding  $H_{01}$  is rejected. It is interpreted that male employee are contributing more in combating cybercrime as compared to male students /teachers.

$H_{02}$ :- There is no significant difference in opinions of female employees and female students /teachers for the techniques in combating cybercrime.

Table 4: Mean, SD and CR ratio

| Variables                 | N   | Means | SD.  | DF. | CR.   | Level of Significance                            |
|---------------------------|-----|-------|------|-----|-------|--|
| Female Employees          | 70  | 70.30 | 5.44 | 168 | 12.15 | Significant at .05 and .01 level of significance |
| Female Students/ Teachers | 100 | 59.00 | 6.67 |     |       |  |

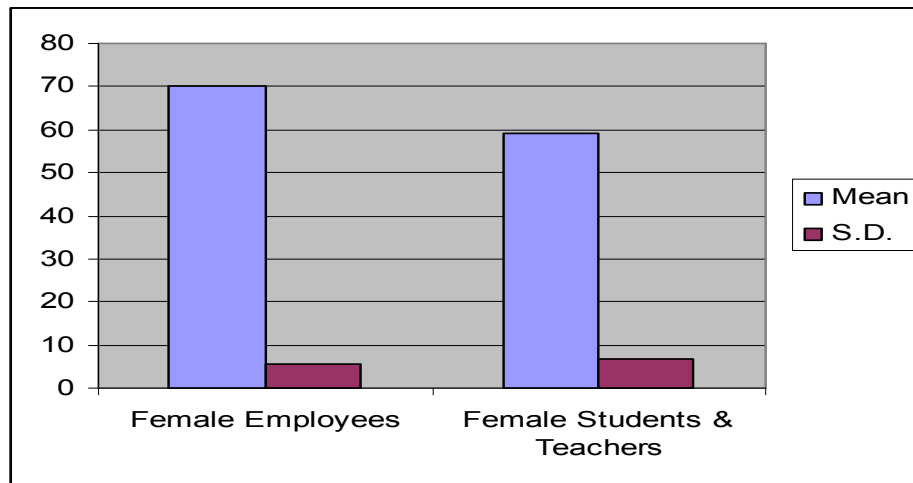


Figure 2 Techniques in combating cybercrime (female)

Table 4 indicates that the mean scores of opinions of female employee for the techniques in combating cybercrime is 70.30 and the mean score of opinions for the techniques in female student /teacher in combating cybercrime is 59.00 and their SD values are 5.44 and 6.67 respectively. The CR value comes out to be 12.15 which is significant at .05 and .01 level of significance at DF value = 168. This further reveals that the two groups differ significantly because the table value at DF = 168 are 1.98 at .05 level of significance and 2.61 at 0.01 level of significance are lower than the calculated value; see figure 2. It is concluded that female employee and female student/teachers differ significantly and the mean value of opinions for the techniques in female employees are greater than female students/teachers. Therefore it is analyzed that the female employees are contributing more in combating cybercrime than female students/teachers. The corresponding  $H_0$  is rejected. It is interpreted that female employees are contributing more in combating cybercrime as compared to female students/teachers.

H<sub>03</sub>:- There is no significant difference in opinions of female employees and male students/teachers for the techniques in combating cybercrime.

Table 5: Mean, SD and CR ratio

| Variables                | N   | Means | SD    | DF  | CR   | Level of Significance                                |
|--------------------------|-----|-------|-------|-----|------|--|
| Female Employees         | 70  | 70.30 | 5.44  | 218 | 1.77 | Non significant at .05 and .01 level of significance |
| Male Students / Teachers | 150 | 73.25 | 18.76 |     |      |  |

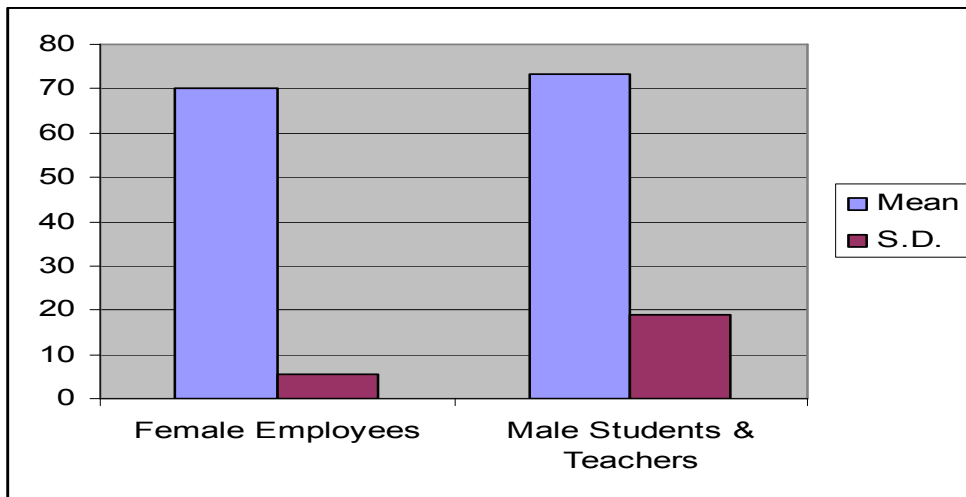


Figure 3 Techniques for combating cybercrime (female vs. male)

Table 5 indicates that the mean scores of female employees in combating cybercrime is 7.30 and the mean score of male students/teachers in combating cybercrime is 73.25 and their SD values are 5.44 and 18.76 respectively. The CR value comes out to be 1.77 which is significant at .05 and .01 level of significance at DF value = 218. This further reveals that the two groups are significantly same because the table value at DF =218 are 1.97 at .05 level of significance and 2.60 at 0.01 level of significance are slightly greater than the calculated value; See figure 3. It is concluded that female employees and male students/teachers group significantly same and the mean value of male students/teachers is slightly greater than female employees .Therefore it is analyzed that the opinions of male students/teachers and female employees are same in combating

cybercrime. The corresponding  $H_{03}$  is accepted. It is interpreted that male students/teachers and female employees are nearly same in combating cybercrime.

$H_{04}$ :- There is no significant difference in opinions of male employees and female students /teachers in combating cybercrime.

Table 6: Mean, SD and CR ratio

| Variables                  | N   | Means | SD.   | DF. | CR.   | Level of Significance |
|----------------------------|-----|-------|-------|-----|-------|-----------------------|
| Male Employees             | 80  | 85.32 | 16.87 | 178 | 13.22 | Significant           |
| Female Students / Teachers | 100 | 59.00 | 6.67  |     |       |                       |

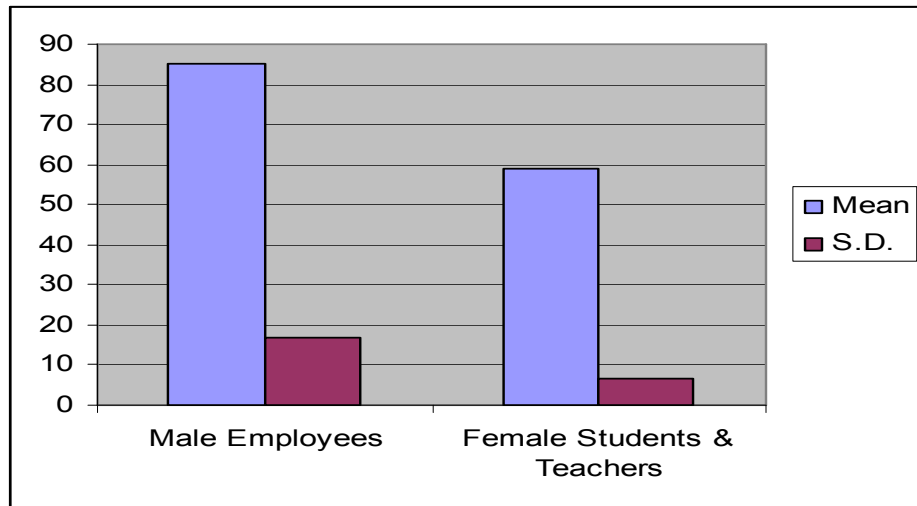


Figure 4 Techniques for combating cybercrime (male vs. female)

Table 6 indicates that the mean scores of male employees in combating cyber crime is 85.32 and the mean score of female students/teachers in combating cybercrime is 59.00 and their SD values are 16.87 and 6.67 respectively. The CR value comes out to be 13.22 which is significant at .05 and .01 level of significance at DF value = 178. This further reveals that the two groups differ significantly because the table value at DF =178 are 1.98 at .05 level of significance and 2.61 at 0.01 level of significance are lower than the calculated value. It is concluded that male employees and female students/teachers differ significantly and the mean value of male employees is greater than female students/teachers. Therefore it is analyzed that the male employees are combating more against cybercrime than female students/teachers. The corresponding  $H_{04}$  is rejected. It is



interpreted that male employees are more in combating cybercrime as compare to female students/teachers.

## V.CONCLUSION

The findings of this research were based on analysis and interpretation of data which supported the objective and hypotheses formulated in this research. The  $H_{01}$  was said to be null hypothesis and was rejected.. The inference was drawn that male employees are more interested combating cybercrime.  $H_{02}$  was also said to be null hypothesis hence rejected because there was significant difference of opinions for the techniques in combating cybercrime between female employees and female students/teachers. It was further concluded that female employees were more interested in combating cybercrime. The  $H_{03}$  was accepted. It was concluded that the female employee and male students /teachers all were equally interested in combating cyber crime.  $H_{04}$  was rejected. It was concluded that the male employees are more interested combating cybercrime as compared to female students/teachers..

## REFERENCES

- Geetha, B. (2011), Vulnerable in virtual space, *The Tribune*, Retrieved from [www.tribune.india.com/2011/20111107/edit.htm](http://www.tribune.india.com/2011/20111107/edit.htm) on August 7, 2012
- Untila, A. (2012), Current methods combating cybercrime. *ITU News*. Retrieved from <https://itunews.itu.int/En/2473-Combating-cybercrime.note.aspx> on August 12, 2012.
- Munyua, A. et al. (n.d.), Women and cybercrime in Kenya: the dark side of ICTS, Retrieved from <http://www.nbo.icann.org> on August 16, 2012.
- CCRC (2005), UN recommendations on fighting cybercrime. Retrieved from: <http://www.crime-research.org/news/13.5.2005/1225> on August 13, 2012
- Casey, E. (2000), Digital Evidence and Computer Crime San Diego: *Academic Press*.Retrieved from <http://books.google.co.in/books>.on August 20, 2012
- Yar, M. (2005), The Novelty of 'Cyber crime': An Assessment in Light of Routine Activity Theory *European Journal of Criminology*, Volume 2 (4): 407–427: doi: 10.1177/147737080556056

Clark, R.(2004), Technology, criminology and crime science. *European Journal on Criminal Policy and Research*, 10(1), pp. 55–63,. Retrieved from <http://books.google.co.in/books>.on August 20, 2012

Toyne, S. (2003), Scam targets NatWest customers. *BBCNews Online*, Retrieved from <http://news.bbc.co.uk/1/hi/business/3211635.htm>. on August 22, 2012