Cyber Crime Prevention and Role of Libraries

Vinay Kumar D.

ABSTRACT
The concept of cyber crime or cyber attack which was more known in the Western world is making its presence in developing countries like India. There has been an increase in Internet accessibility and in the last few years which could pose a serious problem for the Internet users. India is in a step forward to tackle the situation. In this context, the purpose of this paper is to review the current scenario of supportive issued to the increase in cyber crime in India and the probable attempts to prevent such crimes. This paper also emphasizes on the role of academic library in guiding its user community to prevent the white collar crimes.


INTRODUCTION
India is a fastest growing Internet using country in the world especially in Asia. Companies like BSNL, MTNL, Airtel, Reliance etc. are providing internet service at the competitive rates. 3G and 4G revolution in mobile phone industry brought internet access now on mobile phones at higher speed. The successive support from the Indian government to the application of broadband facility in mobile phones also results in the increased use of Internet.

The Internet usage momentum is not only from the side of desktop computers, it is also by the side of mobile internet users. Internet and Mobile Association of India [IAMAI] and market research leader IMRB reported that there were 46 million mobile Internet users in India in September, 2011, whereas, the number is increased to 143.2 million by March 2013. However, a total of 164.81 million net connections stand in India, Abudheen. Along with the mobile Internet connections, the popularity of cyber cafes is also growing which has resulted in the increased use of Internet in India. India is a major market for Internet products and services in the 21st century. The growing information needs for various purposes encourage the use of Internet and www. The web itself has both advantages and disadvantages. The youth of India is attracted to Internet in general and social networking sites in particular in order to communicate, post personnel information to the larger audience.

The advantages of the Internet are all that people enjoy to access all kinds of information anytime from anywhere; transformation and expansion of trade and business, electronic governance, e-learning and education, research, entertainment, culture, etc. 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.

These harmful products of the Internet need to be included under the strong purview of the law, and need time to get sorted out. India is not exempted from the Internet crimes. The explosive growth of social networking sites in India, the rising popularity of mobile devices offering them and the ease of putting personal content on the Web have fuelled a rise in cyber stalking, fake profiles and offences that emerge on the pages social networking sites, Sharma.

As usage of the Internet continues to grow, and with it the realization that there exists countless individuals with the capacity and intent to use the medium to inflict damage, the world finds itself racing to secure legislation that will protect the incredible assets that are now stored online.

Highly populated countries in Asia like China, India are depended on web resources in order to compensate their
information requirements. On the other hand, it creates opportunity to commit crimes in this platform. It is also highly difficult to detect and prevent Internet crimes in widely scattered networking environment. In this regard Indian government strives towards in preventing the cyber crimes by enacting Information Technology Act, 2000.

PROBABLE MEASURES TO PREVENT CYBER CRIMES

- Cyber Laws and Information Security
  
  India passed the Information Technology Act 2000 in May 2000 and notified it for effectiveness on October 17, 2000. The act has also been amended in 2008 and presently known as IT (amendment) act, 2008 and was notified for enactment on October 27, 2009. The sections 65-74 of the acts deal with the punishment for the cyber crimes.

- Online Awareness Programs
  
  Information security awareness is provided through the websites in India. Department of Information technology, Government of India has launched a website to create awareness to the public, http://deity.gov.in/content/cyber-laws-security. Information security awareness for children, students and parents has been provided through this website.

- Cyber Crime Cells
  
  India has nine cyber crime cells actively working in Mumbai, Chennai, Bangalore, Hyderabad, Delhi, Thane, Pune, Gujarat and Gurgaon which involved in investigating the cyber attacks (as of 2013).

- Inclusion of Concept in the Syllabus
  
  In India education is growing sector. Computer education has been made compulsory in primary and higher education level. Although, there are 500 and more Universities and their constituent colleges imparting education in various disciplines, very little percentage of computer threat issues including information security issues were taught in Indian education system, there is an urgent need of inclusion of information security issues, cyber crime awareness courses in the curriculum of colleges and universities.

- Responsibilities of the Police Department
  
  IT (amendment) act, 2008 of India offers any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government to enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence. Police department in this regard must be very clear about the suspects. Also they may conduct awareness programs to make public Internet crime literate8.

- Role of Media in Creating Awareness
  
  Media could play an important role in terms of informing people that computer crime exists and instilling an awareness of the different types of crimes. In India, there are more than 100 news channels broadcasting news in different languages. News channels are the major resource to spread the news to lay man. This could be the useful media in creating awareness about the crimes committed over the web platform.

ROLE OF ACADEMIC LIBRARIES

Academic libraries are the one who subscribe e-resources in large number, Hadagali4, Mulla5. At par with the e-resources, libraries are creating user databases, hold and maintain the catalogue database. These data should be secured from the unauthorized users of the library.

Students, teaching community, are highly dependent on the e-resources which are subscribed by the institutional libraries. Users of the university and college libraries are involved in accessing large number of e-resources. Libraries are the sensitive place where user may face cyber attacks or might commit Internet crimes. It is the responsibilities of libraries to provide user education in relation with secure access to online information.

The following security measures should be followed in the libraries to protect huge amount of information. The same can be informed to the library users to protect the libraries from being attacked by cyber criminals.

- Not to create contact with strangers over the Internet
- Using updated antivirus software in order to protect the library data from virus, malwares.
- Knowing the sources of cyber crimes
- Not to share passwords and credit card details at the time of online transactions, if any.
- Taking up the regular data backups
- Use of firewalls
- Promoting user authentication methods (user name and password, biometrics) while providing access to library data.

The methods followed to protect valuable data and to prevent cyber attacks should be well defined and implemented in the library setup, Zimerman11.

CONCLUSION

Internet access is gaining momentum in the information society. It also allows the criminals to commit crimes in the networked environment. Cyber crime is emerging as a serious threat. The governments, police departments and intelligence units have started to react to prevent this crime Gandhi3. Initiatives have been taken by the government departments to prevent the white collar crime. Cyber cells in the metropolitan cities of India have been established. They are actively involved in educating the people. Present day academic libraries along with the public libraries need to be conscious in this regard. Sources of the cybercrimes should be known and the same information should be transferred to the public of the society and students, teachers of the academic institutions, who spent huge amount of time over the Internet.

REFERENCES


5. http://indiacyberlab.in


