ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2015; 1(8): 21-24
www.allresearchjournal.com
Received: 18-05-2015
Accepted: 23-06-2015

Dr. NK Bhuvaneswari
Research Associate, Centre for Women's Studies, Alagappa University, Karaikudi, Tamil Nadu.

Dr. KR Murugan
Associate Professor and Director i/c, Centre for Women's Studies, Alagappa University, Karaikudi, Tamil Nadu.

Correspondence:
Dr. NK Bhuvaneswari
Research Associate, Centre for Women's Studies, Alagappa University, Karaikudi, Tamil Nadu.

Nature and impact of cybercrime against girls

NK Bhuvaneswari, KR Murugan

Abstract
Cybercrime is one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, internet auction fraud, the penetration of online financial services, as well as the deployment of viruses and various email scams such as phishing. Children especially girls are highly vulnerable to cybercrime and this is an issue of serious concern. Both parents and children need to be educated on how to be cyber smart and they need to be made aware of what is appropriate to share online. Also they should learn about using the internet wisely. Issues like cyber bullying and cyber stalking need to be addressed. The internet is not a scary place, but it is misused. In other words, in the digital age our virtual identities are essential elements of everyday life, we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Hence, the study tries to examine the present scenario of cybercrime and to find out the preventive measures to eliminate cybercrime among girls that should be taken up to protect themselves.

Keywords: Girls, Internet, Social Networks, Cyber Space, Cybercrime,

1. Introduction
"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".
– National Research Council, "computers at risk", 1991

The internet, as we know, has grown rapidly over the last decade. It has given rise to many avenues in every field we can think of – be it education, entertainment, business, or sports. However with every boon there is a curse too. This curse is cybercrime – illegal activities committed over the internet. The internet, along with its advantages, has also exposed us 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 over internet are on the rise.

2. Cybercrime
Cybercrime is a term used broadly to describe criminal activity in which computers or networks are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories. Although the term cybercrime is usually restricted to describing criminal activity in which the computer or network is an essential part of the crime, this term is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.
Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified. This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled.

3. Characteristics of cybercrime
- Commission of an illegal act using a computer, its systems, or applications
- Unlawful acts wherein the computer is either a tool or a target or both

- Crimes perpetrated in computer environment
- Criminals are young and smart with technology
- Trans-national /interstate criminals
- Strong audit trail
- Veil of anonymity

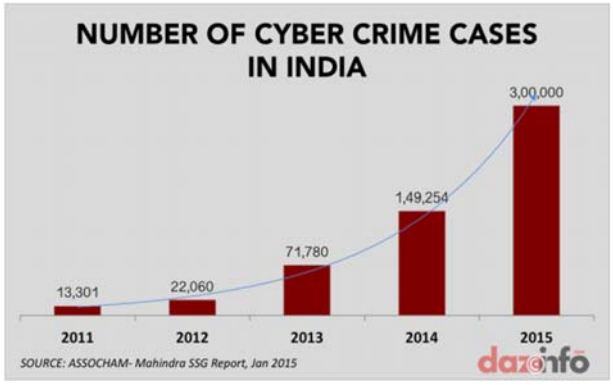
4. Six common types of cybercrime

As the internet, mobile phones, and other computer technologies have flourished, criminals have found ways to use them for old-fashioned goals such as theft, fraud, intimidation, and harassment. Crimes committed through the use of computer systems are known as cybercrimes. Here are some common cybercrimes to look out for.

- Fraud
- Computer trespassing
- Hardware hijacking
- Bullying, harassment, and stalking
- Spam
- Information warfare

5. Cybercrimes on the rise

Cybercrimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cybercrimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes.



6. Statement of the problem

Cybercrime is the latest and perhaps the most complicated problem in the cyber world that requires active mitigation strategies by the society, government, families and individuals. There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities. The growing problem of cybercrime is an important issue facing researchers today. The number of internet users has grown exponentially over the last twenty years. However, it is really only in the last decade that researchers have really begun to study the problem. The purpose of this study is to take a look at the nature and impact of cybercrime against girls.

7. Significance of the study

The increased reliance of individuals/organizations on cyberspace has resulted in corresponding increase in the cybercrimes. Coupled with lack of proper training and education, the low level of awareness of the Indian society about the cybercrime has resulted into a spurt of cybercrimes. At times, even the law enforcement officers do not have proper training and other requisite expertise for tackling cybercrime. India may succeed in combating the problem of cybercrimes by adopting a synergetic approach wherein technological measures and proper legislative framework to combat cybercrime in the society. Hence there is need to enhance awareness about the cybercrime. The growing danger by cybercrime in India needs technological, behavioral and legal awareness; and proper education and training. The study being reported herein examines the awareness of netizens about cyber laws and role of police.

8. Research Methodology

8.1 Objectives of the study

- To assess the awareness about cybercrime among girls
- To investigate the nature of cybercrime against girls
- To explore difference forms of cybercrime affects girls
- To analyze the impact of media on cybercrime against girls
- To identify ideal strategies to prevent cybercrime against girls.

8.2 Research Design

The present study is descriptive and analytical in nature based on empirical data relating to cybercrime against girls collected from the study universe through a closed and open ended questionnaire

8.3 Study universe

To find out the nature and impact of cybercrime against College girls in Karaikudi, one of the colleges in Karaikudi was selected through lot system in which Alagappa Chettiar college of engineering and technology is selected for the study.

8.4 Sampling

There are five branches (i.e. civil engineering, mechanical engineering, electrical and electronics engineering, electronics and communication engineering and computer science engineering) in Alagappa Chettiar College of engineering and technology in which 20 students each in the respective departments of the college randomly. Hence, stratified random sampling technique is adopted for the study.

8.5 Data collection

The primary sources mainly include empirical data directly collected from the respondents, documents and records available with the national crime records bureau and government functionaries. The secondary sources comprise of published books, articles available both from national and international journals and newspapers besides various cybercrime related websites.

8.6 Data processing

Collected data have been processed through SPSS (Statistical Package for Social Sciences) for interpretation.

9 Findings of the study

The findings of the study are as follows

- In the study, half of the respondents are belonged to the age group of 20.

- Caste ascribes the social status of an individual on the basis of her/his birth. It is observed that 55% of the respondents are belonged to backward community, caste is an important social phenomenon in the Indian context.
- Religion plays a major role in influencing the habits, thinking and attitudes of people. Majority (96%) of the respondents belongs to the Hindu religion,
- 53% of the respondents are using internet for social networking in the study.
- Regarding the accessibility, (86%) of the respondents has internet access on their own.
- More than half of the respondents are using laptop for internet access.
- Half of the respondents are using Wi-Fi connection for internet.
- It is revealed that 27% of the respondents are using internet every day.
- Also, it is noted that half (53%) of the respondents is using internet for social networking.
- Most (52%) of the respondents are using trail version of anti-virus to secure their system.
- Half of (50%) the respondents are visiting education related websites in the internet.
- The majority (65%) of the respondents is searching subject oriented information through internet.
- Majority (73%) of the respondents trusts the information supply through online surfing.
- It is found that 72% of the respondents have known about cyber-crime
- It is noted that the majority (87%) of the respondents is not affected by cybercrime in the study area.
- It is found that 34% of the respondents have social network account user id with duplicate name
- The majority of 82% of the respondents said that they are not revealing their personal details with online friends.
- It is found that 97% of the respondents are not received any messages/posts/chat from fake id.
- It is noticeable fact that 57% of the respondents are not interested in communicating/chatting with other unknown person.
- More than half of the respondents revealed that they exchange ideas with one another via online chatting.
- It is inferred that 76% of the respondents said that hacking has been made by using software.
- The majority of 92% of the respondents said that they have not been hacked by someone in the study.
- It is noted that 79% of them are not using the credit/ debit card as payment method.
- It is inferred that 51% of the respondents said that the media creates awareness about cybercrime
- Majority of 40% of the respondents said that the media influence people to involve in criminal activities.
- It is found that 49% of the respondents felt that awareness about the cybercrime and cyber law is needed to prevent cybercrime
- It is noted that 79% of the respondents have not been known about cyber law
- It is found that the majority of 81% of the respondents are not aware of cybercrime cell in Tamil Nadu
- It is found that 37% of the respondents said that creating awareness about cybercrime and safety education against cybercrime is needed to eliminate cybercrime

10 Ideal Strategies to prevent Cybercrime

- Use anti-virus and spyware detectors/cleaners regularly.
- Make Backups of Important Files and Folders to protect important files and records from the computer
- Use tough passwords but easy to remember and difficult to guess.
- Use a variety of passwords and not same for all of the accounts.
- Beware of spam legitimate looking email asking for confidential information. Never ever click on the link given in the spam email.
- Always delete spam emails immediately and empty the trash box to prevent accidental clicking on the same link.
- Be cautious about the websites that require your card details before you actually place an order.
- Not to believe everything we read online.

11. Conclusion

Prevention is always better than cure. It is always better to take certain precaution while operating the net. It is significant to improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest. One should never post personal information online or share sensitive information such as your social security number and credit card number. Exercise caution when clicking on any links or downloading any programs. Although protecting ourselves does take some effort, remember that there are a lot of resources and tools to help us. And by adopting a few precautions and best practices, we can help keep cybercrime from growing. In order to implement effective prevention strategies, it is imperative that educators, parents, and legislators understand the motivation behind the occurrence of cybercrime.

12. References

1. Bagyavati. Social engineering in lech j.janczewski and andrew m.colarik cyber warefare and cyber terrorism, 2009.
2. Bargavi, sheeba. Safety issues in orkut for girls, unpublished, November, 2009.
3. Belsey, bill. Examples of cyber bullying. www.cyberbullying.org. Web. 28 Nov. 2011. <http://www.cyberbullying.org/examples.html>.
4. Bradley. Predators on social networks, 2009.
5. Brenner. Social networking dangers exposed, 2009.
6. Brunker m. sexting surprise: teens face child porn charges, 6 pa. High school students busted after sharing nude photos via cell phones. Retrieved on 26th January 2010, 2009. from http://www.msnbc.msn.com/id/28679588/cert annual report 2010
7. Collier and magid social networking dangers in perspective, 2009.
8. http://library.thinkquest.org/06aug/02257/
9. http://ncrb.nic.in/cd-cii2011/statistics2011.pdf
10. http://tech2.in.com/news/general/1791-cyber-crime-cases-registered-in-india-in-2011/322162
11. http://technology.inquirer.net/19074/over-1-5m-are-cybercrime-victims-daily-worldwide-study
12. http://udini.proquest.com/view/understanding-cybercrime-a-goid:848940191/
13. http://www.cybercrimejournal.com/editorialijccjan2009.pdf

14. http://www.cyberlawtimes.com/articles/103.html
15. http://www.informationweek.com/news/internet/social_network/showarticle.jhtml?articleid=219500360
16. Http://www.infosecurity-magazine.com/view/2503/social-networking-a-risk-to-information-security/
17. http://www.legalindia.in/cyber-crimes-and-the-law
18. http://www.naavi.org/cl_editorial_11/edit_sept_10_norton_cyber_crime_report.htm
19. Http://www.networkworld.com/news/2009/020909-slapped-in-the-facebook-social.html
20. http://www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/cybercrime_study_210213.pdf