Strategies to Prevent and Control of Cybercrime against Women and Girls

S.Poulpunitha, K.Manimekalai, P.Veeramani

Abstract: ***The emergence of ICT has provided an unrivalled opportunity for women to exploit their capabilities to improve their quality of life as well as to contribute to the welfare of the society. Internet has also become a social and communication tool with e-mails being an efficient communication tool. Internet offers new possibilities for networking and participative democracy but feminists are failing to challenge the use of the Internet for furthering more dangerous and discriminatory agendas, including Internet crime committed against women and the proliferation of pornography. Many youth are engaging socially through common social network like WhatsApp, Facebook, twitter, msn, my space and are actually addicted to these Internet social activities, making them vulnerable to Internet crimes. The increased dependency of individual / organisations on cyberspace has led to the increase in the cybercrimes. In India we find there is minimal proper training and education regarding such developments and the ignorance towards these advancements has paved way for cybercrimes. Even the authorities and officers who handle such cases have no proper training and the essential expertise for undertaking cybercrimes against women and girls in particular. India should consider adopting a coactive approach wherein technology and proper legislative framework combine to fight the cybercrime in the society. The threatening atmosphere created by such heinous cybercrimes against women and girls need radical change in technology, behaviour and legal affairs; facilitated by proper education and training. This study examines the problems and issues of cybercrime against women and girls in order to exhibit preventive strategies and means to fight back with the support of cohesive forces.***

Keywords: ***Cybercrime, Awareness, Education, Law enforcement, Preventive measures***

I. INTRODUCTION

Cybercrime has become a term associated only with women in India, though globally deals with non-monetary offenses. In majority of cases the victim invariably becomes women, who fall prey to technological fancies. India is one of the very few countries to enact IT Act 2000 to combat cybercrimes, but issues involving women are still grievously continued. This Act strictly terms offenses as hacking, publishing of obscene materials on the net, tampering the data as punishable offenses. But yet the gravest exploitation and danger to the security of women in general is not addressed by this Act.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author

Dr.S.Poulpunitha*, Assistant Professor,Department Women'sStudies, Alagappa University, Karaikudi.

Prof.K.Manimekalai, Professor& Head Department Women's Studies, Alagappa University, Karaikudi.

Dr.P.Veeramani, Assistant Professor, Department Women'sStudies, Alagappa University, Karaikudi.

Protection of women has always been a concern especially in a country like India. Crime rates in India have seen a steep increase in years. Women felt insecure in places outside home earlier, but today home is one of the major places for women where they are being victimized. With technology and internet becoming the parallel form of living women don't feel safe anymore, anywhere. Its effects are worse for them and on the society as a whole. Many websites and blogs have taken up the issues of cybercrime to create awareness for the safety of women and children in the net. Yet the crime rates in this area are higher, and pose a major setback for the development of the nation

Statement of the Problem

Cybercrime is the alarming concern which has sprung in recent times and perhaps it is the most complicated problem in the cyber world that requires immediate attention and promising strategies from the society, government, families and individuals. Limited authenticated and reliable statistics on the nature of crime and the monetary loss of the victims are available for reference, almost of these crimes are never brought into record. A specific and effective study on the occurrence and avoidance of such disturbing cybercrimes would be a good area of research today. Over the last two decades the usage of internet has taken a giant leap. However, researchers have begun to study such cases and problems only in the later years. The purpose of this study deals the nature and kinds of cybercrimes against women and girls, how women can be protected from these crime and what steps could be taken to prevent them.

RESEARCH METHODOLOGY

Objectives

- ➢ To assess the awareness about cybercrime among women and girls
- ➢ To investigate the nature of cybercrime among women and girls
- ➢ To identify ideal strategies to prevent cybercrime against women and girls

Universe of the study

The study has been carried out from affiliated colleges of Alagappa University in Sivaganga and Ramnad Districts

Sampling Design

Multistage sampling method has been adopted to investigate the cybercrime against women and girls.

Sampling Size

Out of 45 affiliated colleges of Alagappa University, 2 government colleges for women working under Alagappa University have been chosen for the study. Further 50 samples have been selected from each of two colleges, totally 100 samples have been selected for the research study.

II. RESULT AND DISCUSSION

Purpose of internet usage

Purpose of internet	Frequency	Percent
Internet banking	11	11.0
Shopping	16	16.0
Research	21	21.0
General information	13	13.0
E-mail	21	21.0
Social networking	53	53.0

(Multiple responses)

The different types of usage of the internet connection are internet banking, shopping, research, general information, social networking and others. The above table shows that 21% of the respondents use internet connection, for the purpose of research and e-mail respectively, 11% of the respondents use internet for the purpose of internet banking, 16%of the respondents use internet for the purpose of shopping, 13% of the respondents use internet for collecting general information. The majority (53%) of the respondents use internet for social networking.

A. Way to girls are affected by cybercrime

Particulars	Frequency	Percent
Their accounts are hacked in social network	38	38.0
Details have been duplicated/misused/hacking of personal details	21	21.0
Facing real time problem	53	53.0
Threatening/forced to do unwanted work	25	25.0
Lack of awareness about the crime	81	81.0
Mental torcher/psychological problem	22	22.0
Photo morphing/misusing photos	32	32.0
Illegal access of girls accounts	15	15.0
Using social network / face book	54	54.0
Using internet cafe	3	3.0
Fake accounts	2	2.0

(Multiple responses)

From the above table, it is noted that majority 81% of them said that the girls are affected due to the lack of awareness about the cybercrime. 38% of the respondents said that girls account have been hacked in social network.21% of them said that the girl's personal details have been hacked and 53% of them felt that they are facing real time problems in their life and 54%of the respondents said that the girls are affected by social network accounts.25% of the respondents said that the girls are threatened to do unwanted work and 22% of the respondents said that the girls are affected by psychological problem and 32% of the respondents said that the girls are affected by photo morphing in social network. Also 15% of them said that the girls account is accessed illegally without the knowledge of them.The remaining 3%, 2% of them felt that the girls are affected by cybercafé and also by fake accounts respectively

B. Strategy needed to prevent this type of cyber crime

Aspects	Frequency	Percent
Awareness about the cybercrime & cyber law	49	49.0
Report to concern authority	8	8.0
Introduce cyber-safety education curriculum	24	24.0
Research is need to prevent from the crime	3	3.0
Automate software updated	4	4.0
Awareness about the cybercrime & cyber safety education	5	5.0
Awareness about the cybercrime report to concern authority	4	4.0
Cyber safety education, research, automat software update	3	3.0
Total	**100**	**100**

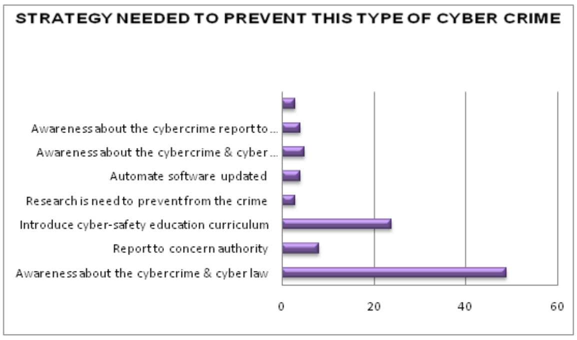

Figure: 1 Strategy Needed To Prevent This Type of Cyber Crime

The above table shows the alarming issues that need immediate attention to prevent cybercrime. Majority of 49% of the respondents felt that awareness about the cybercrime and cyber law is needed to prevent cybercrime, 24% of them said that education curriculum should encompass cyber safety measures for the students, 8% of the respondents said that the victims should report to the concern authorities, 3% and 4% of them felt that research is needed to combat cybercrime and automate software updates should be available for the netizens respectively. Also 5% of them felt that awareness about cybercrime and cyber safety education is needed to prevent cybercrime. 4% of the respondents said that awareness about cybercrime and cyber law and also the cybercrime victims should report to the concerned authorities, the remaining 3% of them said that cyber safety should be imparted in education Crime research is needed in order to prevent cybercrime and automated software update is also needed to prevent cybercrime against girls.

Major Findings

- It is inferred that the majority (86%) of the respondents have internet access on their own.
- The majority (62%) of the respondents use laptop for internet access.
- It is inferred (53%) of the respondents use Wi-Fi connection for internet.
- The half (53%) of the respondents is using internet for social networking.
- It is revealed that the majority (82%) of the respondents said that they installed anti-virus software in their system
- The half of (50%) the respondents are visiting education related websites in the internet.
- The majority (65%) of the respondents is searching subject oriented information in the internet.
- The majority (73%) of the respondents trusts the information supply through online surfing
- It is noted 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 revealed that 64% of the respondents are said that they do not prefer online chatting
- It is noticeable facts that 57% of the respondents are not interest communicate/chat with other unknown person.
- It is found that the majority of 60% of the respondents said 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 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

III. STRATEGIES TO PREVENT CYBERCRIME

- A coactive approach involving the initiatives and steps taken by the Government and other legislative bodies to address such crimes would be the best way to tackle these cybercrimes
- To avoid cyber stalking it is advisable not to disclose any personal information online.
- Sending personal pictures online to friends and strangers during chat has been seen a major cause for crimes against women. Refraining from such acts is essential
- It is cautious to keep the credit and debit card details confidential at any cost. Reliable sources should be checked in case of genuine transaction
- Empower and educate women and children with adequate knowledge and awareness about the occurrence of such gross crimes in the society to keep them protected and safe
- Firewalls serve as a great first line of defense when it comes to checking such trespasses. Ensure the safe use of security checks. Always enable the firewall that comes with your router
- Exercise caution and Presence of mind in dealing with such threats. Do not fall prey to fancies
- Become aware of the legal framework and proceedings that are connected to such crimes, in order to take action immediately when trapped
- Be well informed about the advancements in the technology and internet to stay unharmed

V. CONCLUSION

The research shows that only few users are not aware about cybercrime. There are ample number of tools and resources available to sort such matters of concerns. Adopting few preventive measures and best practices, we can surely keep cybercrime at bay. To implement more effective prevention strategies, it is mandatory that educators, parents, law enforcement, and legislators understand the root cause of the occurrence of such cybercrimes. Schools and colleges should regularly educate both students and parents on safe surfing, through workshops and seminars. Awareness of cybercrime should be a part of regular course work in educational institutions.The free internet facilities provided to educational institutions should be carefully monitored and kept secure. Cyber cells and cyber court assigned to deal such proceedings should be increased in number. Productive tie ups between IT companies and law enforcement authorities may help in tracking and penalizing individuals who indulge in such crimes.

ACKNOWLEDGEMENT

I gratefully acknowledge the funding support received from the National Commission for Women (NCW), New Delhi and we would like to thank my colleagues from the Department of Women's Studies, Alagappa University who have extended their commendable and unwavering help for the completion of this paper.

REFERENCES

1. Bagyavati (2009) 'social engineering' in lech j.janczewski and andrew m.colarik cyber warefare and cyber terrorism
2. Bargavi and sheeba (2009 November) 'safety issues in orkut for girls', unpublished.
3. Brunker, m. (2009). '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.
4. Dittrich, dave. "the "stacheldraht" distributed denial of service attack tool." University of Washington. University of Washington, 31 Dec. 1999. Web. 28 Nov. 2011.
5. High technology crime investigation association. "2010 report on cybercrime investigation." high technology crime investigation association. Htcia, inc., 2010. Web. 28 Nov. 2011.
6. Nature and impact of cybercrime against college girls in karaikudi, Published Centre for Women's Studies, 2013
7. Snell, p.a. and e.k. Englander, 2010. Cyber bullying victimization and behaviors among girls: applying research findings in the field. J. Soc. Sci., Asian social science, vol. 8, no. 15; 2012, Canadian centre of science and education
8. http://www.telegraph.co.uk/technology/apple/8914975/black-friday-itunes-credit-scam.html>.
9.
10. http://www.legalindia.in/cyber-crimes-and-the-law
11. http://www.naavi.org/cl_editorial_11/edit_sept_10_norton_cyber_crime_report.htm
12. http://www.net-security.org/secworld.php?id=15127
13. http://www.cyberbullying.org/examples.html>.
14. http://www.ovc.gov/publications/bulletins/internet_2_2001/ncj184931.pdf
15. http://www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/cybercrime_study_210213.pdf
16. http://www.unodc.org/documents/organizedcrime/unodc_ccpcj_eg.4_2013/cybercrime_study_210213.pdf
17. http://zeenews.india.com/exclusive/30-key-crime-facts-about-india_6418.html
18. www.ccsenet.org/ass
19. www.messagelabs.com

AUTHORS PROFILE

Dr.S.Poulpunitha, Assistant Professor, Department of Women's Studies Alagappa University, Karaikudi. She has 12 years of experience in teaching and Research Activities. She has published more than 20 publications as books, articles and research reports. Her area of specialization is Violence against Women, Women Empowerment, and Gender and Development. She has more than 27 paper presented in various national and international conferences.

Prof. K. Manimekalai, Head, Department of Women's Studies and Director, Centre for Women's Studies, Alagappa University, Karaikudi. Also, she was Former Vice-Chancellor, Mother Teresa Women's University, Kodaikanal, former Registrer and former Dean, AlagappaUniversity. She has produced a number of M.Phil and Ph.D candidates. She has published more than 50 publications as books, articles and research reports. Her area of specialization is Women Empowerment, Gender and Development and Women Entreprenurship. She has completed 15 research projects sponsored by National and International agencies. She has been bestowed with several honors and awards.

Dr.P.Veeramani is working as a Assistant Professor, Department of Women's Studies, Alagappa University. She has 12 years of experience in teaching and Research Activities. She has published 33 articles in the National and International Journals and Books. She has 42 Presented the papers in International, National and State level Conferences.