IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 11, November 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011059|

Cyber Crimes against Women

Dr. Neeta Gupta[1], Dr. Vandana Gaur[2]

Associate Professor, Dept. of Psychology, D.A.V. (PG) College, Dehradun, India[1]

Assistant Professor, Dept. of Psychology, S.D.M. Govt. PG College, Doiwala, Dehradun, India [2]

ABSTRACT: Information Technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to easier, speedy, efficient, and time saving method of transactions. Various criminals like hackers, crackers have also found ways and measures to interfere with the internet accounts and have been successful in gaining unauthorized access to the user's computer system and stolen useful data.

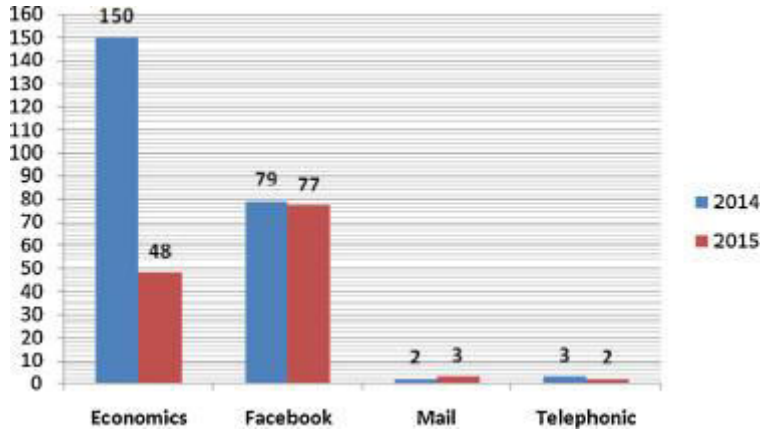
The proliferation of e-mail as the preferred method of communication has given rise to various issues of concern to the legislators and employers alike. By its very nature, email encourages people to be frank and open in the discussion and given the ease with which it is composed and sent, people are ordinarily not as careful on the email as they would have been, if they had committed the contents of email to the letter. Harassment via email, includes black mailing, threatening and constant sending of love letters in anonymous names or regular sending of embarrassing mails. Email is capable of performing all the functions of a normal mail (or 'snail- mail' as it has been dubbed.)

Section 67 of the Information Technology Act makes publication, transmission and causing to be transmitted and published in electronic form any material containing sexually explicit act or conduct, punishable. Publishing and transmitting cyber pornography via instant messaging, emails or any other mode of digital transmission is an offence. In my opinion online pornography should be completely banned as it is responsible for declining values and sexual permissiveness leading to sex crimes against women and children. As many of these pornographic sites depict women and children as sex objects, demeaning their position and showing them as passive recipients of degrading and/or violent acts leading to unrealistic and artificial expectations and various forms of physical, mental and sexual abuse. These unrealistic and artificial representations often pressures the victims to enact or consent to acts which they find demeaning having negative mental and psychological health outcomes and consequences.

KEYWORDS: cyber crime, women, india, harassment , sex, punishment

I. INTRODUCTION

The expanding reach of information technology has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. However, the means that enable the free flow of information and ideas over long distances also give rise to a worryingly high incidence of irresponsible behavior towards women. Any technological development is capable of beneficial uses as well as misuse.[1]



Internet Crimes

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

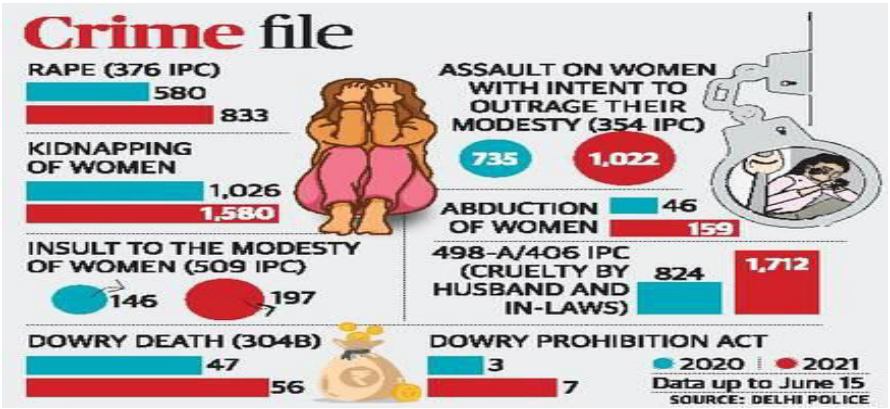
| DOI:10.15680/IJIRSET.2021.1011059|

It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment. The present study is an attempt to highlight the cyber-crimes against women in India. The economic, political and social conditions of these countries are different to each other. Moreover, the problem against women is also treated of the same nature worldwide. The study throws light on the types of cyber crimes against women in India in the light of Information Technology Act, 2000. And viz-a-viz the problems and loopholes behind dealing with Cyber Crimes against Women. [2]

Information technology has widened itself over the last two decades and has become the axis of todays global and technical development. The world of internet provides every user all the required information fastest communication and sharing tool making it the most valuable source of information. With the numerous advancement of internet, the crime using internet has also widened its roots in all directions. [3]

Cyber Crime Negative Impacts On Women

The cyber-crimes pose a great threat to individuals. Cyber-crime is a global phenomenon and women are the soft targets of this new form of crime. Cyber-crime is emerging as a challenge for national and economic security. Cyber Stalking, Harassment via Email, Cyber Defamation, Morphing, and Email Spoofing against women are the basic cyber crimes.[4]



Crime file against women

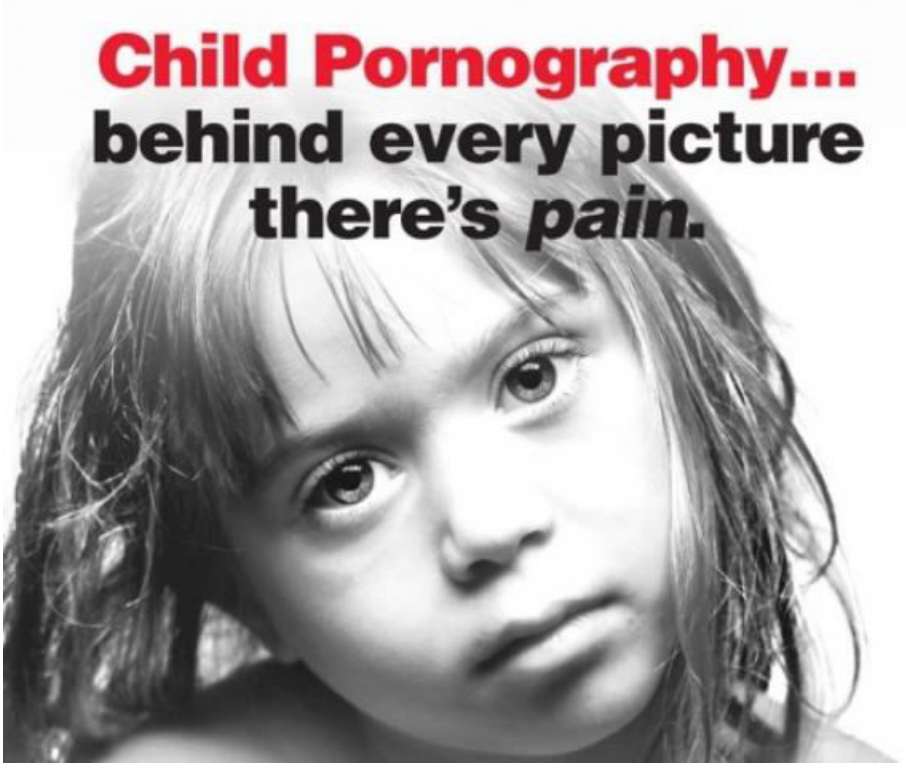
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011059|

II. OBSERVATIONS

- Harassment through e-mails: Harassment via email, includes black mailing, threatening and constant sending of love letters in anonymous names or regular sending of embarrassing mails.[5]
- Cyber stalking: 'Stalkers are strengthened by the anonymity the internet offers. He may be on the other side of the earth, or a next door neighbor or a near relative!' It involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. In general, the stalker intends to cause emotional distress and has no legitimate purpose to his communications.[6]
- Cyber defamation: Cyber defamation also called Cyber smearing can be understood as the intentional infringement of 'another person's right to his good name. 'Cyber Defamation occurs with the help of computers and / or the Internet. It is considered more of a menace owing to its expeditious nature.[7]
- Child pornography: Child sexually abusive material (CSAM) refers to material containing sexual image in any form, of a child who is abused or sexually exploited. Section 67 (B) of IT Act states that "it is punishable for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.[8]



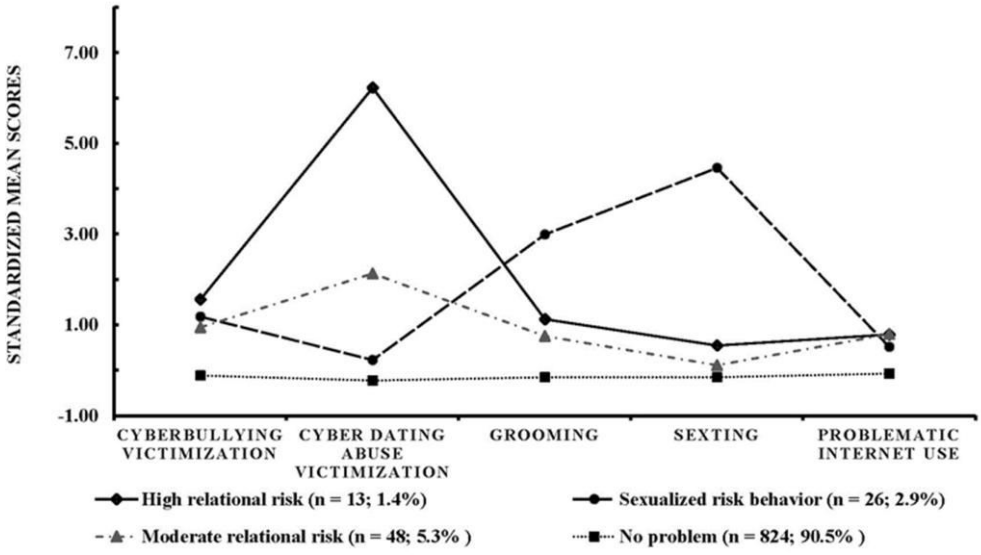
- Cyber bullying: A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011059|

- Cyber grooming: Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.
- Chapter XI of the IT Act deals with the offences such as tampering with computer source documents.[2]
- Section 65 deals with hacking of computer system.
- Section 66 deals with publishing of information which is obscene in electric form.
- Section 67 deals with Access to protected system.
- Section 70 deals with Breach of confidentiality and privacy.[9]



III. DISCUSSION

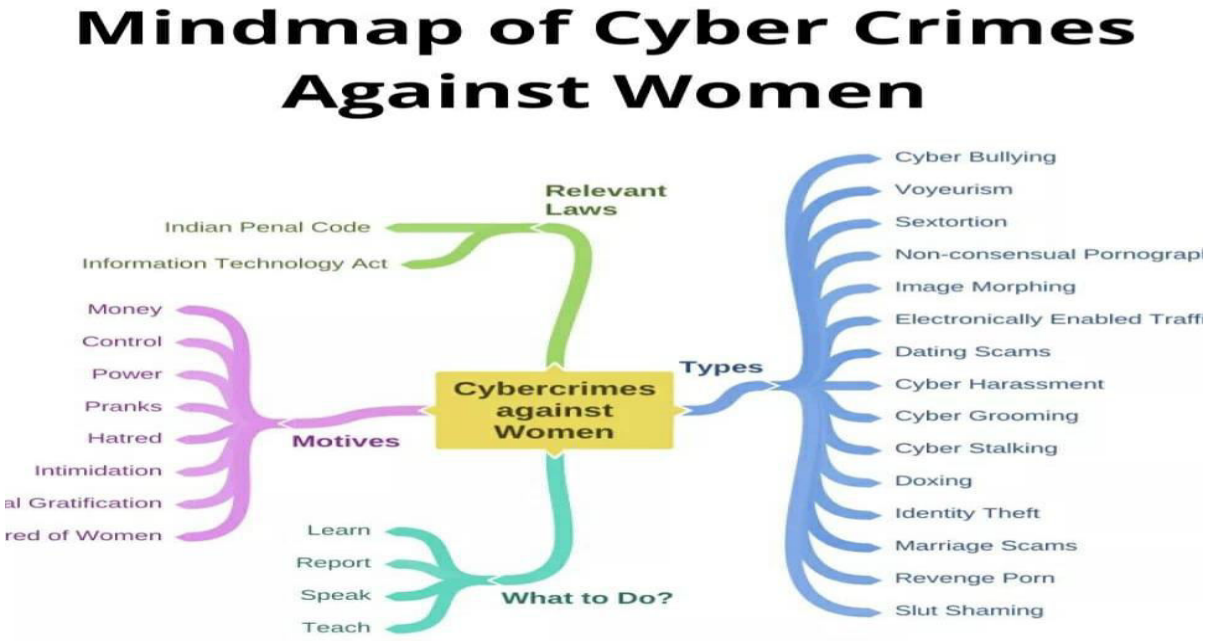
- In case of cyber- crimes, a victim may contact the nearest cyber cell or police station.[4]
- A complaint may also be filed anonymously through National Cyber crime Reporting Portal (cyber crime.gov.in).
- To file a complaint alleging commission of a cyber-crime the following documents must be provided:
- In case of hacking the following information should be provided: Server logs.
    - Soft copy as well as hard copy of defaced web page in case your website is defaced.
    - In case the data is compromised on your server or computer or any other network equipment, soft copy of original data and compromised data is required.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011059 |

- Access control mechanism details i.e. who had what kind of the access to the compromised system.[10]
- List of suspects if any.
- All relevant information leading to the answers to following questions
  - What has been compromised in the system?
  - Who might have compromised the system?
  - When the system was compromised?
  - Why the system might have been compromised?
  - Where is the impact of attack-identifying the target system from the network?
  - How many systems have been compromised by the attack?
- In case of e-mail abuse like vulgar e-mails, etc., the following information should be provided:
  - Extract the extended headers of offending e-mail and bring soft copy as well as hard copy of offending e-mail.
  - Please do not delete the offending e-mail from your e-mail box.
  - Please save the copy of offending e-mail on your computer's hard drive.[11]



IV. RESULTS

Online safety should be maintained

- Keep an eye out for irrelevant / fraudulent phone/email messages.
- Don't respond to email messages that ask for personal information.
- Be aware of fraudulent Websites used to steal personal information.
- Pay attention to privacy policies on Websites and in software .
- Guard your email address.
- Use Strong Passwords.[12]

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011059|

Figure 1.7: Possible underlying factors linked to increases in cybercrime

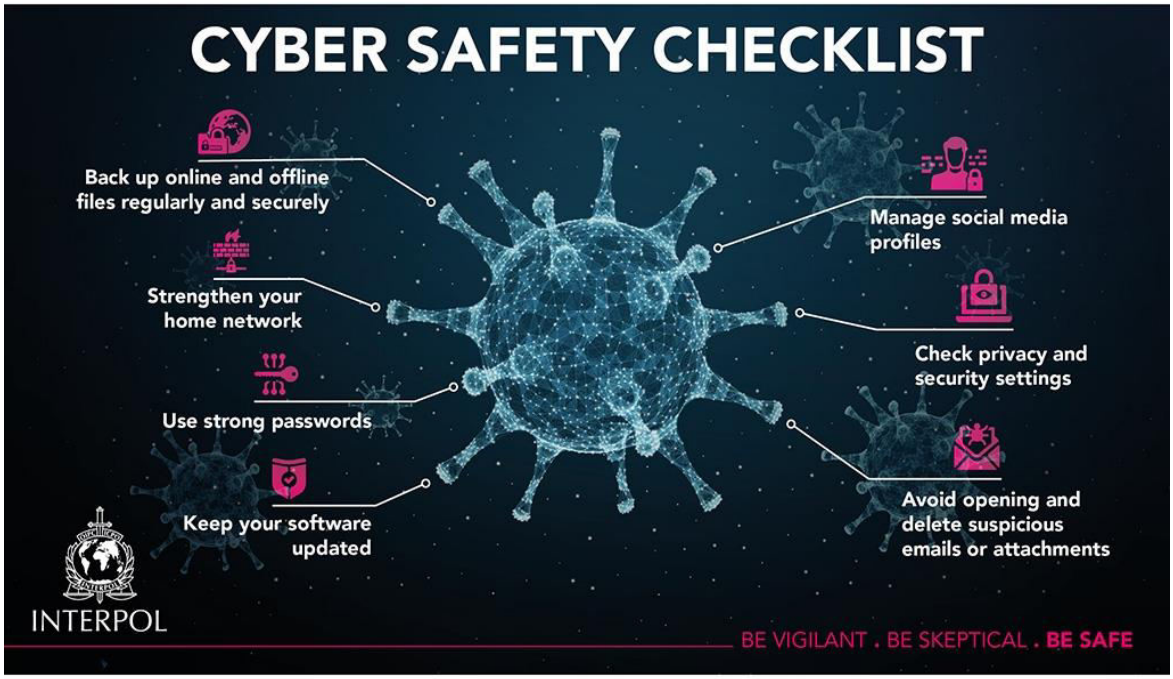
1. Don't share passwords.
It may sound silly. Who in their right mind shares their password, right?
Wrong. You may have shared your password with a trusted friend or partner. According to the Norton CyberCrime Report two in three people believe it's riskier to share their email password with a friend than lend them their car. The fear is reasonable. While friends may not intentionally cause you harm, they may accidently reveal your password to someone. Sometimes relationships change before your password does. Use your discretion and keep those passwords private and complicated.[13]
2. Don't leave your webcam connected.
There are too many apps capable of turning on your camera and slyly recording your movements without your knowledge. As a precaution disable camera permission and keep the lens of your camera closed or covered when not in use.
3. Don't share more than necessary.
Relationships have only two shades in a spectrum – very good or very bad. Even the best of people can swing from one end of the spectrum to the other. That is why use caution when you share intimate messages, pictures, information or anything that has the potential to come back and embarrass you.
4. Don't meet online acquaintances alone.
Always let your friends and family know where you are going and who you are meeting. Make sure you meet the person in a crowded coffee shop or mall.[6]
5 Reveal only as much as needed.
There are too many sinister characters browsing social media sites to initiate friendship with unsuspecting women. Be careful about posting details about your whereabouts and lifestyle. Stalkers can find ways to reach you with a simple photograph or status update. Disable geotagging in your camera. Enable it only when required. Any device with an enabled 'location service' poses the risk of exposing your exact location at any given time.[14]
6. Update all operating systems on you devices.
They can be nuisance. But they are very important to keep you safe. Security updates and patches keep the latest threats away. Always install them no matter how busy you are.[8]
7. Secure your devices with anti-virus software
Having a mobile phone or a tablet without a security system in place is like sitting in a house with the doors unlocked. Both android and mac devices are at risk from malicious software invading and taking over your life. Always install a reliable security system like Norton Security in all your devices.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011059|

8.Read the fine print
Know and understand the privacy policy and terms of service of any service you use. Some websites can own, sell, rent or resell your information to anyone they want. This can come back as a bigger problem and the law may not be able protect you since you agreed to the terms and conditions.[10]
9. There is no such thing as 'freebies'
Freebies come as games, offers, deals, etc. They may be riddled with viruses, spyware and malicious software. These can get into your device and mine all your data.
10. Block people you don't want to interact with
Never feel weird declining friend requests from people you barely know. Trust your instinct and ignore, unfriend or block them. You get to choose who stays on your friend list.
When it comes to safety, both online and offline, common sense is the first line of defense. Your instincts play a critical role in your protection. If something feels 'off', go with your instincts. You don't have to explain your reasoning to anyone.[12]



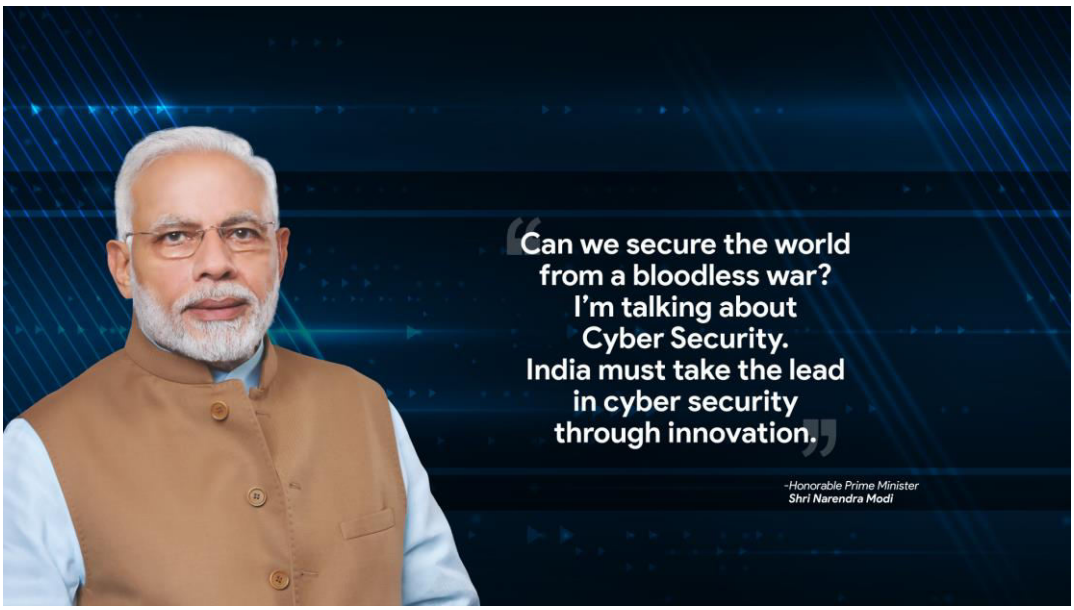
V. CONCLUSION

The National Commission for Women has, in collaboration with the Facebook and Cyber Peace Foundation (a civil society organisation based in Ranchi, Jharkhand involved in training related to all aspects of cyber security), initiated a 'Digital Literacy Programme' for college/ university students. The programme seeks promoting digital literacy for women including the precautions that can be taken; raising awareness about cyber crimes; and advising the users about the resources available to women; to prevent the problems and also how to handle such crimes. The "Digital Literacy and Online Safety Programme" aims to train 60,000 women in universities across major cities of India regarding safe use of internet, social media and email that will enable them to differentiate between the credible and questionable information available online. The programme, in its initial phase, is o to cover the states of Punjab, Manipur, Haryana, Meghalaya, Delhi-NCR, Sikkim, Maharashtra and Tamil Nadu. The program was launched on 18th June, 2018 at Punjab University, Chandigarh in the presence of Hon'ble Governor of Haryana.[14]

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 11, November 2021 ||

| DOI:10.15680/IJIRSET.2021.1011059|



REFERENCES

1. The word "Cyber Space" was coined by "William Gibson," the Canadian/American science fiction writer who helped define its cyberpunk sub-genre, in 1982 in his novelette "Burning Chrome" in Omni magazine, and in his novel "Neuromancer".
2. The Cambridge English Dictionary defines Cybercrimes as crimes committed with the use of computers or relating to computer, especially through Internet.
3. (2008) 3 MLJ (Crl) 578.
4. (2004) also available at www.naavi.org/cl_editorial_04/suhas_katti_case.htm.
5. http://www.mailsbroadcast.com/e-email.broadcast.faq/46.email.spoofing.htm.
6. G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007)
7. Section 66 of Information Technology Act, 2000.
8 .Abhimanyu Behera, " Cyber Crimes and Law In India," XXXI, IJCC 19 (2010)
9. G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007)
10. According to Oxford Dictionary
11. Available at http://blog.koldcast.tv/2011/koldcast-news/8- infamous-cases-of-cyber-bullying/
12.http://trak.in/tags/business/2010/04/07/internet-usage-indiareport-2010/
13. Abhimanyu Behera, " Cyber Crimes and Law In India," XXXI, IJCC 19 (2010)
14. http://www.genderit.org/es/node/2213)

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details