IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
A Multidisciplinary Double-Blind Peer Reviewed Refereed Monthly Journal
Volume 2, Issue 2, October 2022
Impact Factor: 6.252

Cyber Crimes and Cyber Hygiene Practices Among Young Girls

Dr. K. Kanchana[1], Ms. Afiya Begum Y[2], Ms. Dhejas M[3] and Ms. Jothi J[4]
M. Com., Ph.D., (NET & SET)[1]
Assistant Professor, Department of B. Com (Corporate Secretaryship)[1]
Students, III B. Com (Corporate Secretaryship)[2,3,4]
Chevalier T. Thomas Elizabeth College for Women, Chennai, Tamil Nadu, India

Abstract: *The world evidences an immense transformation from pen & paper culture to digital culture, particularly, post covid pandemic. We live in the digitally complex generation. The evolution of digitalization and explosive usage of internet have lead to cyber crimes (e-crimes) and cyber violations. With the increase of 'Work from Home' option, women are more prone to serious consequences of cyber attacks and lead to traumatic experiences. The Government of India has started attempting to renovate our nation into digitally enabled and empowered, through its "The Digital India" project. But, is the digitalization completely favourable for our people? The primary aim of the study is to answer this question by creating awareness on cyber crimes and security measures among women and young girls, whom the law looks down and does not recognize properly, even in today's developed society. An attempt is made to keep them away from any sort harm by cyber usage or exploitations. In the direction to caution women about cyber threats by not hindering digitalization and innovation, the authors have analyzed previous research studies conducted with respect to cyber threats and security space, major cyber crime cases in India, Cyber laws, agencies that deal with cyber security and key initiatives implemented by our Indian government to protect innocent people from cyber threats. Hence, at the end of this study, protective measures and cyber hygiene practices are suggested to make women and young girls become more cautious and reorient their behaviour to make safest use of internet and protect themselves against cyber attacks.*

Keywords: Cyber Crime, Cyber Security, Cyber Law, etc.

I. INTRODUCTION

The Introduction of computers has made the life of human beings easier, the computer has been using for various purpose from an individual to big Organisations across the globe. Most computer user's are utilising computers and using advance technology for their personal benefits or any other Organisational goals. And this gave a birth to cybercrime. Cyber crime means any crimes or offence incurred using the computers or Information system is known as cybercrime, and the Law which control or resign over the cyber space. In Modern World, the right to use the Internet has become Human rights, as declared by the Union Nations Human Rights Council in June 2016. Simultaneously, this gave birth to a large number of internet users growing rapidly in India and across the World India is developing rapidly and one of the major factor contributing to its growth is Technological advancement. India step ahead with advancements in the science and Technology department and particularly, the Information Technology.

Yet, this rapid advancement has its lens kilion too. The Citizens, women in spot of more susceptible to criminal activities carried out by usage of Internet, which is referred as cybercrimes. Cyber crime is usually committed by cyber criminals on leaders who want to make money. Cyber crimes are committed by Individuals or Organisations. It includes Phishing scams, Online scams, Malware, E-mail bombing, virus dissemination, login bombs, Theft, social media hack and spoofing, sales and important fraud etc , goes on. During the period of lockdown, People's are browsing social media, websites such as Facebook, Instagram, Twitter, and more often watching movies and watching series by subscribing to their web channels like Netflix, Hotstar, Amazon, Voot, Zee etc., and also entertain in online gamers by installing different applications especially women due to various factors such as lack of privacy, unawareness etc, are lead to such cyber attacks in the internet. A study of internet users in India, conducted by the Bonston Consulting group and Retailers Association in India, state that approximately 29% of the users in India are Women. And one cannot deny

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
A Multidisciplinary Double-Blind Peer Reviewed Refereed Monthly Journal
Volume 2, Issue 2, October 2022
Impact Factor: 6.252

the fact that women in our society are prove to cyber crime attacks and offences every now and then, which is a very serious thing to talk about it. With the Advancement of technology, Cyber crimes and victimization of women are increasing and at give a great threat to the security and mental health of a woman. And India is one of the Nations to exact and enforce the legislation to combat the cyber crimes especially against the women. Cybercrimes against women in India is still taken lightly, people must learn that they should not interface in one's personal lives of others, and should have a respect towards women, Hence, to avoid or eradicate cyber crime against women in India, Strict legal penal reforms and policies should be introduced and not only that but also a change in education system is a huge requirement. This study was undertaken on the observation of Cyber Security Awareness month – October.

II. LITERATURE REVIEW

Sanjeev kumar & Priyanka [2019] in their research cyber crime against women: Right To Privacy And Other Issues has stated that women are viewed and portrayed as sex objects, she is treated inferior to men in various societal spheres and functions; this has created a huge gender bias between the men and women where even the men think that their wrongdoings towards women cannot be penalized.

And he has stated that the job of the legal system and regulatory agencies to keep pace with the technological developments and ensure that newer technologies do not become tools of exploitation and harassment.

Animesh Singh And Ankita Rathi [2017] in their research current scenario of cyber crime in India has stated that with increase in the use of internet services , the cyber crime has been increasing .cyber crime is not only limited to India and has be increasing globally due to the high reliance on the internet services .The Government is constantly taking initiatives to reduce cyber crime from India but is still lacking in doing so .All the countries should unite globally and work together to curb the cyber crime . Government of every country is working on it to curb the crime but it will be effective if multiple country joins together to curb the crime.

III. OBJECTIVES

- To suggest and provide in-depth knowledge on the concept of cyber crime and cyber security against young girls
- To identify the common form of cyber crimes threatening women in recent days
- To provide suggestive measures to curb cyber crime against women and young girls all over the world.

IV. LIMITATIONS

- This study is based on observation made in a very limited period of time.
- Only 60 female students of 17 to 20 years of age, from particular strata were selected for the observation randomly. So the samples were not evenly and normally distributed. The other way, results might vary.

V. REASONS FOR THE GROWTH OF CYBER CRIME AGAINST WOMEN ARE AS UNDER

- The absolute limit of internet – no limit, never changing
- Low economic cost
- Countless vulnerable targets – loneliness is the primary cause due to which many female students and women stay away from their family for the job / stay for longer period of time over the internet.
- Most of the cyber crimes are not reported due to the fear of the society and hesitation of victim due to fear and family's reputation in the society.

Due to this even today the Indian police does not take cyber crime seriously, In such situation women or female falls for the prey to such cyber crimes should inform their parents and first should approach women assistance cell or NGO such as All Indian Women's Conference, Sakshi navjyoti, Centre for cyber victims counselling they will help and guide them the process, and they also make sure that the police does not take the crime cases lightly. The government of India should make stringent laws and proper implementation of such laws should be amended. They should be accountable and take effective steps to protect women from cyber crime and due to the delay in justice; people have lost faith in the law enforcement and law implementations. Therefore, women should by themselves to must aware of their rights and legal rule to curb cyber crime. There are so many websites and social media applications provides enormous options in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
A Multidisciplinary Double-Blind Peer Reviewed Refereed Monthly Journal
Volume 2, Issue 2, October 2022
Impact Factor: 6.252

their privacy policies to protect the women and at the same time, most of the popular websites declare their privacy policies, that the websites or the applications will not take any responsibilities for any sort of harassment caused or faced by the users. Therefore, women should be careful before registering on the social media websites and apps, and women should carefully go through the privacy policies before registering them in it. Therefore, negligence and carelessness is the root cause is regards to women bring the targets of cyber crime.

VI. SCOPE OF THE STUDY

Cyber Crimes is a new millennium threat to society nowadays which brings by developments of technology and information. Various forms of cybercrimes exist either theft or fraud involving money or property or safety threat involving contamination of dignity. A Cyber can destroy web sites and portals by hacking and planting viruses, play online frauds by transfer of funds from one corner of the globe to another and gain access to highly confidential and sensitive information. Moreover he can cause harassment by e-mail threats or obscene material, play tax frauds, indulge in Cyber pornography involving children, and commit innumerable other crimes on the Internet. With the growing use of the Internet, Cybercrime would affect us all, either directly or indirectly. Hence, awareness among women on cyber crimes and security measures are mandatory.

VII. MOST COMMON CYBER CRIMES AGAINST WOMEN IN THE SOCIETY

Cybercrime is construed as using a computer as a weapon, or instrument, to advance or secure something deemed illegal. Think stealing identities or intellectual property, committing fraud, or violating privacy laws. These are just several examples.

Here are 5 of the top cybercrimes affecting businesses and individuals in 2022:

- Phishing Scams to steal personal information and credit card numbers
- Website/ Email Spoofing
- Blackmailing or Threatening in Cyber space
- Cyber Pornography
- Cyber Stalking/ bullying in various social media platforms
- Publishing or Uploading Morphed/ Obscene sexual materials
- Creation of duplicate profile using fake ids to defame the reputation of women
- Identity theft against Right to Privacy under Article 21 of Indian Constitution
- Child Soliciting & Sexual harassment/ Abuse
- Social media hacking and Spamming
- Email bombing
- Copyright Violation
- Unauthorized access to their personal network devices
- Wiretapping to listen to personal conversations

7.1 Phishing Scams

Phishing emails mean messages from someone you know or a business that you trust. They are designed to trick people into giving up personal information or clicking on malicious link that downloads malware. Thousands of phishing attacks are launched every day.

7.2 Website Spoofing

The word spoof means to hoax, trick, or deceive. Website spoofing is when a website is designed to look like a real one and deceive you into believing it is a legitimate site. This is done to gain your confidence, get access to your systems, steal data, steal money, or spread malware. Website spoofing works by replicating a legitimate website with a big company's style, branding, user interface, and even domain name in an attempt to trick users into entering their usernames and passwords. This is how the bad guys capture your data or drop malware onto your computer.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
A Multidisciplinary Double-Blind Peer Reviewed Refereed Monthly Journal
Volume 2, Issue 2, October 2022
Impact Factor: 6.252

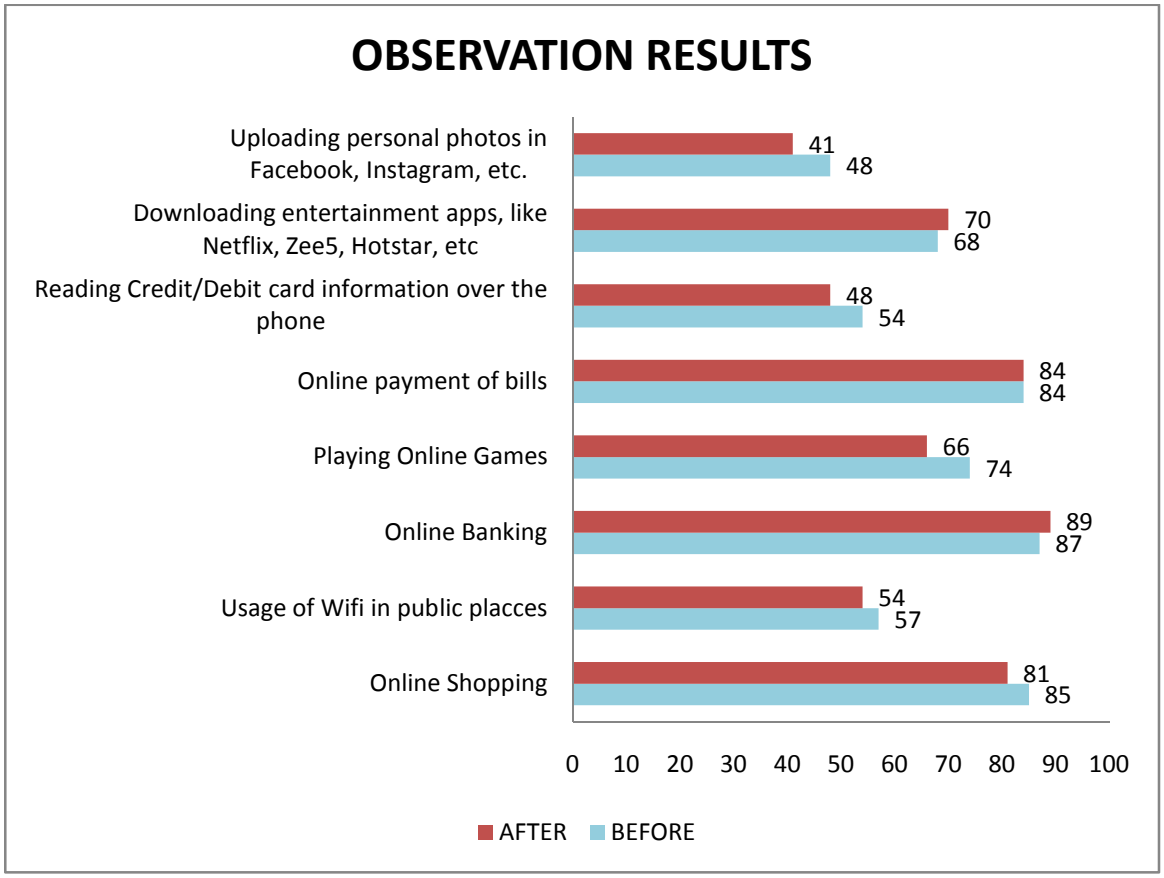
7.3 Malware

Malware as "various software" specifically designed to gain access to or damage a computer. Common types of malware include:

- Viruses that spread, damage functionality, and corrupt files
- Trojans disguised as legitimate software that quietly create backdoors to let other malware into your network
- Worms that can infect all of the devices connected to a network

VIII. RESULTS OF THE OBSERVATION

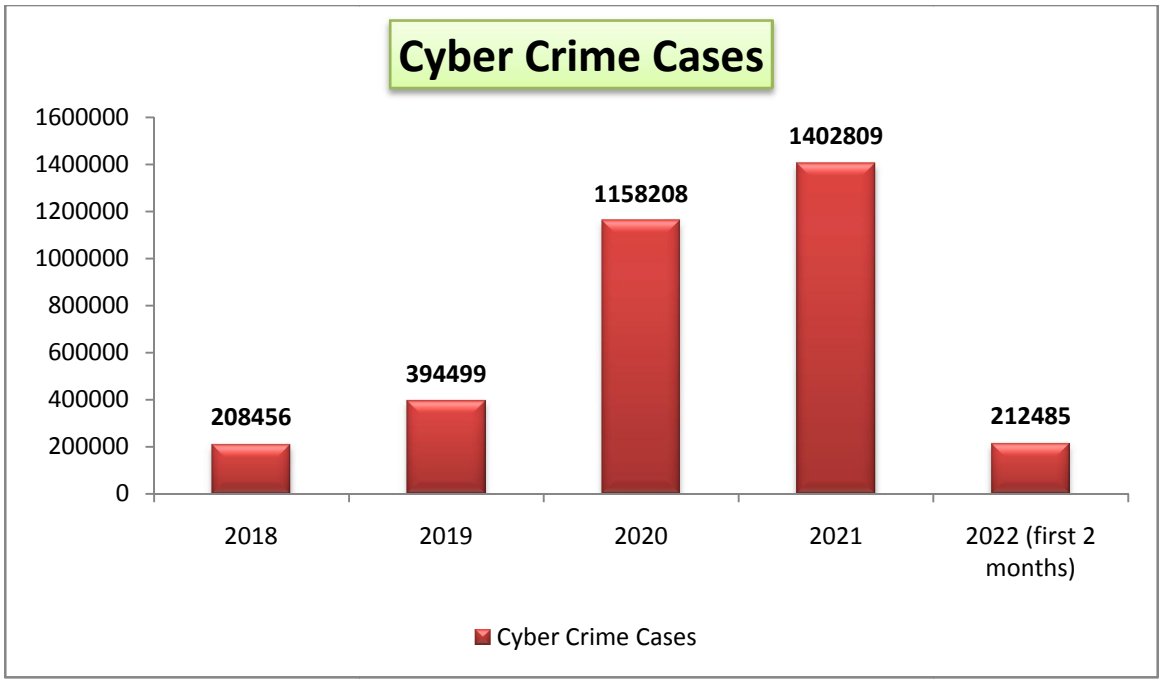
This study was carried out in the month of October, in observation of 'Cyber Security Awareness Month" which is celebrated globally. A Workshop was conducted on Cyber Crime Awareness. An observation was made in the period from September 20, 2022 to October 10, 2022. This study records the behavioural changes among students on cyber space before and after the workshop, with a simple unstructured questionnaire consisted of ten simple close-ended questions related to the usage and awareness level of digital space among students. The result of the observation is presented below in chart form:



NUMBER OF CYBER CRIMES CASES OVER THE YEARS:

The number of cyber crime cases against women has recorded at steeper rate of 28 percent, as per the record of National Crime Records Bureau.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
A Multidisciplinary Double-Blind Peer Reviewed Refereed Monthly Journal
Volume 2, Issue 2, October 2022
Impact Factor: 6.252



Source: CERT-In (Indian Computer Emergency Response Team)

IX. INITIATIVES TAKEN BY INDIAN GOVERNMENT AGAINST CYBER CRIME

In the era of digital world it is necessary to maintain the adequate cyber security measures in today's high technological digital environment to safeguard the information technology for the organisation and also for the environment as well as society. The government of India has taken many initiatives on cyber security.

- **The Indian computer emergency response team,[CERT-IN]:** This [CERT-IN] operates the national agency and also to address the countries cyber security towards organisations as well as society which has helped to reduce the number of rate of cyber attack on government networks.
- **Cyber Surakshit Bharat:** The aim of this scheme is to strengthen the cyber ecosystem in India with the vision of "Digital Trading". This initiative is launched by the information technology [Meity]. This program was in partnership with [NGO] National electronic governance division.
- **National critical information infrastructure protection center [NCIIPC]:** The initiative is to establish by the central government of India in order to protect the critical info act of the company which protects critical info about country on National security growth and public health care.
- **Appointment of chief info security officer:** The government of India has passed a written guideline for the chief info security officer of government organisation to outline the best practice for safeguarding apps and infrastructure where the CISOS can identify and document the security requirements.
- **Personal data protection bill:** The POP bill was first introduced on dec11, 2019 in Loksabha and it was passed with the aim to provide protection in digital privacy relating to personal data and also to create trust between the person and agencies in data processing.
- **Cyber Swachhta Kendra:** The cyber Swachhta Kendra is the initiative taken by digital India to ensure and create cyber space by eliminating the bonnet infection by cleaning the security system of end user prevent cyber infection.
- **National cyber security policy 2013:** The NCSP 2013 is an initiative by the government of India in order to protect the information infrastructure and to facilitate the creation of secure computing environment.
- To enhance awareness about cyber crimes and cyber hygiene practices among students, an easy to understand 'Handbook' for Adolescents & students booklets for the age group of 13 years is formulated by the government and the same book has been made available at https://mha.gov.in/documents/downloads and www.cybercrime.gov.in.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
A Multidisciplinary Double-Blind Peer Reviewed Refereed Monthly Journal
Volume 2, Issue 2, October 2022
Impact Factor: 6.252

- A scheme for Cyber Crime Prevention against Women and Children (CCWC) has been framed by the Ministry of Home Affairs to tackle various cyber crimes inflicted upon women.
- A Twitter account namely "@Cyberdost" has been launched by the government to spread cyber awareness and to offer cyber security tips/updates on regular basis.

X. SUGGESTIVE MEASURES FOR CYBER SECURITY

- Stringent punishment should be adopted by the Government of India to bring to curb this crime from India in order to protect women from cyber crime.
- Women are not able to report cyber crimes immediately as they are not really aware where has to report such crimes or they are not serious about reporting therefore government setup cyber crime police station and cells which deals with cyber crime only.
- Women or the young girls who falls prey to cyber attacks and become victims should approach a women assistance cell or NGOs like Sakshi, Navjyothi, etc. who can assist, guide and counsel them through the process, if they have fear of family defamation or calling police force individually.
- Do not leave the webcam in "ON" or connected mode while not at use.
- Don't use free wifi given by public places like coffee shop, parks, Theme parks, beach, Restaurants etc, because they can easily hack your personal information.
- Do not click on links in email, download files or open attachments in emails or download unnecessary apps like online games, movie apps, etc the acceptance of which may lead to access of personal information by unknown people.
- Do not upload your photos in Social Media like Instagram, Twitter, Facebook, etc. because they can transfer your image into another image easily by Morphing.
- Awareness about cybercrime and cyber hygiene needs to be introduced in the early stages of education and a proper cyber crime mechanism to be implemented in schools and colleges.
- Women's safety is the most alarming topic not just in India as the crime against women has been rising day by day all over the world. Therefore, Government has introduced Top 17 women safety apps in order to curb cyber crime and women can make use of them.
- Women and children should be educated about the acceptable usage of internet and they are experiencing any kind of online harassment, stalking or bullying and make sure that they are informing their parents or report to cyber crime police station or cells.
- Beware of fraudulent website who takes your personal information like credit/debit card details etc., and keep a watch on irrelevant or fraudulent messages or e-mails and avoid responding them.
- Women should be educated and updated about cyber laws and policies which protect women against cyber crime.
- Awareness about cyber crime and cyber hygienic should be introduced in schools in the early stage of education as a component of student curriculum.
- Strong passwords are vital to good online security. Make your password using a combination of capital and lower-case letters, numbers and symbols, using two-factor authentication.
- Firewalls are effectively gatekeepers between your computer and the internet.
- Get acquainted with available online portals to lodge complaint cyber crimes.
- Personalize your data access to the internet to retain control in the browser.
- Do not blindly click on "Accept" button for the queries raised by third party service providers, which might open access to your contacts, camera, etc.

XI. CONCLUSION

Cybercrime is one of the most deadliest and dangerous crimes of the world. Cybercrime is more difficult to define and deal. It's easy to commit but very difficult to mend. It's a crime of one of the most complex nature. Some of the categories of cybercrime are definitely resemble with traditional crimes, but some are entirely new like cyber stalking,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
A Multidisciplinary Double-Blind Peer Reviewed Refereed Monthly Journal
Volume 2, Issue 2, October 2022
Impact Factor: 6.252

internet phishing. Cyber law is constantly being evolved. As new and new opportunities and challenges are surfacing, cyber law, being a constantly evolving process, is suitably modifying itself to fit the call of the time. Though, information technology act, 2000, itself is a comprehensive legislation but it has had some inherent shortcomings. Cyber law is likely to see various emerging trends that will have to be appropriately addressed by law makers keeping in view the safety of women and young girls of the nation.

REFERENCES

[1]. Halder, D., & Jaishankar, K. (2016). *Cyber crimes against women in India*. SAGE Publications India.

[2]. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on Cyber Crime and Cyber Law's of India. *International Research Journal of Engineering and Technology (IRJET)*, *4*(6), 1633-1640.

[3]. Chowbe, V. S. (2011). The Concept of Cyber-Crime: Nature & Scope. *Available at SSRN 1766238*.

[4]. Shah, M. R. (2019). Cyber Crimes in India: Trends and Prevention. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *6*(1), 25-37.

[5]. Kumar, S., & Manhas, A. (2021). CYBER CRIMES IN INDIA: TRENDS AND PREVENTION. *Galaxy International Interdisciplinary Research Journal*, *9*(05), 363-370.

[6]. Singh, A., & Rathi, A. (2021). Current Scenario of Cyber Crime in India. *Issue 1 Int'l JL Mgmt. & Human.*, *4*, 739.

[7]. Bhongale, D., & Kumar, J. (2021). Crime against women in cyber world. *Crime against Women in Cyber World (August 12, 2021)*.

[8]. https://www.dnaindia.com/technology/report-two-months-of-2022-had-more-cyber-crimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb-2949145

[9]. https://pib.gov.in/PressReleasePage.aspx?PRID=1808686