Changing Trends in Online Abuse and Trafficking of Women and Children

A Study in Jharkhand, Madhya Pradesh, Rajasthan and West Bengal

Space2Grow and CyberPeace Foundation | October 2022
Some Quotes from Study Participants During Field Interviews...

“Through this interview I have realised that the government and civil society are taking steps to address cyber crimes and abuse against women and children...”

“We need to be alert and put all our faculties to use while using the internet in this digital age...”

“We enable cyber criminals to carry on with their activities due to lack of information and awareness. Awareness is thus the need of the hour, especially among students, children and women...”

“People in rural areas lack awareness on issues related to internet usage and therefore fall victim to cybercrimes easily...”

“I have been victimised online so many times that I want young girls to stay away from strangers online...”
# Table of Contents

List of Tables 04

List of Graphs 05

Acknowledgements 06

Executive Summary 09

Introduction to the Research Study 12

A. Scope of the Study
B. Need and Purpose of the Study
C. Research Design and Methodology
D. Limitations of the Study

A Review of Literature on Online Abuse and Trafficking in India 17

A. Cyber Security Risks of Children in Virtual Learning Spaces and Gaming Portals
B. Cyber Violence Against Women and Children
C. Regional Snapshot of Cybercrimes against Women and Children
D. Challenges in Combating Cyber Crimes
E. Roundup of the Literature Review

Trends in Online Abuse and Trafficking of Women and Children: Study Findings 32

A. Profile of the study participants
B. Data on internet usage
C. Experience of cyber fraud and abuse among study participants
D. Knowledge, Perception and Practices: Participants in Cyberspace
E. Qualitative findings from the study

Recommendations of the Study 64

Conclusion 72

References 74

Appendix 81
## List of Tables

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Number of study participants per age group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2</td>
<td>Number of study participants according to occupation</td>
</tr>
<tr>
<td>Table 3</td>
<td>Hours spent online on a daily basis by participants who use the internet daily</td>
</tr>
<tr>
<td>Table 4</td>
<td>Duration of internet usage of study participants</td>
</tr>
<tr>
<td>Table 5</td>
<td>Purpose/s for surfing the internet among study participants</td>
</tr>
<tr>
<td>Table 6</td>
<td>Time spent online daily by participants: District-wise data</td>
</tr>
<tr>
<td>Table 7</td>
<td>District-wise response to friend requests from unknown persons</td>
</tr>
<tr>
<td>Table 8</td>
<td>District-wise response to personal message received from strangers</td>
</tr>
<tr>
<td>Table 9</td>
<td>District-wise response to a loss as a result of phishing</td>
</tr>
<tr>
<td>Table 10</td>
<td>Nature of uncomfortable online interaction district-wise</td>
</tr>
<tr>
<td>Table 11</td>
<td>Experience of participants with cyber bullying, district and age-group wise</td>
</tr>
<tr>
<td>Table 12</td>
<td>Response to cyberbullying incident</td>
</tr>
<tr>
<td>Table 13</td>
<td>Percentage of those who experienced identity theft age-wise and district-wise</td>
</tr>
<tr>
<td>Table 14</td>
<td>Response to seeing fake profile online</td>
</tr>
<tr>
<td>Table 15</td>
<td>Nature of inappropriate material</td>
</tr>
<tr>
<td>Table 16</td>
<td>Person participants confided in regarding uncomfortable online interaction</td>
</tr>
<tr>
<td>Table 17</td>
<td>Participants’ perception of response of parents/spouse to any online abuse/fraud they may face</td>
</tr>
<tr>
<td>Table 18</td>
<td>Reason/s for parental/spousal disapproval to internet/device usage by participants</td>
</tr>
<tr>
<td>Table 19</td>
<td>Reasons for children and women being more vulnerable to online abuse as per participants' perception</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Table 20</td>
<td>Type of exploitation post online interactions</td>
</tr>
</tbody>
</table>

**List of Graphs**

<table>
<thead>
<tr>
<th>Graph 1</th>
<th>Feeling of discomfort during an online interaction, district-wise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph 2</td>
<td>Response of participants to uncomfortable online interaction, district-wise</td>
</tr>
<tr>
<td>Graph 3</td>
<td>Participants’ experience of exposure to inappropriate content, district-wise</td>
</tr>
<tr>
<td>Graph 4</td>
<td>District and age-wise participants’ experience with being stalked online</td>
</tr>
<tr>
<td>Graph 5</td>
<td>Disadvantages of the internet according to study participants</td>
</tr>
<tr>
<td>Graph 6</td>
<td>Participants’ knowledge of abuse/fraud experiences among acquaintances</td>
</tr>
<tr>
<td>Graph 7</td>
<td>Consequence of the incident/s of trafficking/exploitation</td>
</tr>
</tbody>
</table>
Acknowledgements

This study is the result of a collaborative effort by Space2Grow and CyberPeace Foundation (CPF). As organisations working in the area of digital safety, both felt that the time was ripe for an exploration into experiences of women and children with cybercrimes, especially in rural India. This is increasingly significant in the post-pandemic phase that is marked by increased exposure to the internet, penetrating different aspects of one’s life, without a concurring capacity building towards safe practices in online actions and interactions.

While being a collaborative effort between these two organisations, the study has been carried out with the support of volunteers outside the fold of Space2Grow and CPF. The field work for the study was conducted through NGOs and CBOs located in the chosen districts under study, except in the case of Bhopal and Raisen districts. We want to acknowledge the support extended by Ms Rita Bhawasar, Principal, GHSS Badi Bareli and Ms Hemlata Parihar, Principal, GHSS Mahatma Gandhi BHEL towards conducting data collection in the districts of Bhopal and Raisen. The data collection team members for the other six districts are mentioned below.

<table>
<thead>
<tr>
<th>South 24 Parganas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organisation:</strong> Goranbose Gram Bikash Kendra</td>
</tr>
<tr>
<td><strong>Coordinator:</strong> Shaswati Mallick</td>
</tr>
<tr>
<td><strong>Data collection team:</strong> Pampa Ghosh, Chaitali Mondal, Chandona Mondal, Piu Mondal, Rajesh Mondal, Kushalika Raptan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jalpaiguri</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organisation:</strong> Jalpaiguri Mahila Kalyan Sangha</td>
</tr>
<tr>
<td><strong>Coordinator:</strong> Raju Saha</td>
</tr>
<tr>
<td><strong>Data collection team:</strong> Abhijit Chakraborty, Dalia Roy, Raju Saha, Poulomi Sutradhar</td>
</tr>
</tbody>
</table>

Changing Trends in Online Abuse and Trafficking of Women and Children 6
<table>
<thead>
<tr>
<th>Location</th>
<th>Organisation</th>
<th>Coordinator</th>
<th>Data collection team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jaipur</td>
<td>Jan Kala Sahitya Manch Sanstha</td>
<td>Imran Gandhi</td>
<td>Manisha Agrawal, Rekha Kandpal, Sameer Khan, Kajal Singh, Rajkumari Singh, Monika Sharma</td>
</tr>
<tr>
<td>Udaipur</td>
<td>Gayatri Seva Sansthan</td>
<td>Ashita Jain</td>
<td>Lalit Singh Chundawat, Sita Jatt, Subhash Joshi, Payal Kaneriya, Happy Tailor</td>
</tr>
<tr>
<td>Deoghar</td>
<td>Chetna Vikas</td>
<td>Rani Kumari</td>
<td>Aftab Alam, Naresh Das, Vijay Kumar Jha, Kiran Kumari, Mishra Monu Mrinal</td>
</tr>
<tr>
<td>Khunti</td>
<td></td>
<td>Pritiwanti Marry Mundri</td>
<td>Durgi Kujur, Khusbu Kumari, Pritiwanti Marry Mundri, Sunita Tiru, Anandini Topno, Renu Tuti</td>
</tr>
</tbody>
</table>
We want to thank the following individuals from Space2Grow and CyberPeace Foundation for their contribution towards this study. We thank Major Vineet Kumar, Founder and President, CPF, for his support and partnership towards the study. Ms Bhawna Goswami, Assistant Trainer (CPF), conducted the data analysis. Ms Chitra Iyer, Co-Founder and CEO, Space2Grow, needs to be commended for envisioning the study towards exploring the experiences of women and children in rural and semi-urban areas with respect to online abuse and fraud, and for her overall supervision of the project. Finally, Ms Vinishya Philip, Lead Public Policy and Research, Space2Grow, designed and executed the research study and drafted the report.

Once again, on behalf of Space2Grow and CyberPeace Foundation, we thank each one of you for bringing this project to fruition.
Executive Summary

The study proposed to explore trends in online abuse and trafficking of women and children and examine their vulnerability to abuse in rural and semi-urban communities in India. A total of eight districts were chosen from the states of Jharkhand (Deoghar and Khunti), Madhya Pradesh (Bhopal and Raisen), Rajasthan (Jaipur and Udaipur) and West Bengal (Jalpaiguri and South 24 Parganas) for the field study. Women and children in the age range of 13 to 35 years were interviewed. The purpose of choosing these locations is the dearth of studies on online experiences of women and children in rural and semi-urban areas of the country.

The study limited its inquiry to questions on the most common forms of online abuse faced by women and children in India today, such as cyber stalking, bullying, phishing, exposure to inappropriate material, cyber grooming and impersonation and identity theft. This does not, however, discount the fact that participants, and women and children in general, could and do experience other forms of fraud and abuse online. The study also threw up findings on how women and children respond to such abuse and how it impacts them.

This report will be relevant and beneficial for all stakeholders who work with women and children—particularly those working towards their protection and development. Needless to say, this will be helpful for those working in the area of cyber crimes in India—government, civil society, industry and technology companies. Researchers, policy makers and students can gain perspective on the issue and prevalence of cyber crimes in rural areas. This report would also be of interest to mental health professionals who work with women and children.

Key Findings of the Study

➔ While cyber abuse and fraud are extremely common among women and children in the study areas, awareness on prevention, reporting and redressal is abysmally low.
➔ Only a minuscule number of study participants who have been subjected to fraud or abuse online have placed an official complaint about or reported the matter to relevant authorities.
Many study participants shared that they often avoided taking any action in response to fraud or abuse simply because they did not know if and what options were available to them.

A vast majority of study respondents chose to confide in their friends, rather than a close family member like a spouse or parents, when they were faced with some uncomfortable situation online.

The findings indicated a certain level of tolerance to cyber abuse in that participants would not consider reporting an incident unless it was grave or involved financial fraud.

While nearly 89% of study participants own a mobile phone, the study found that women and children additionally use devices that belong to their parents, spouses, or even to their workplace/school/college. It is clear that cyber abuse is agnostic to ownership of devices as it can and does happen via any device and medium.

Many study participants expressed that they never reported cybercrimes/fraud as they did not believe it would lead to any substantial result. They seemed to suggest that justice can never be meted out in cases of cyber crime.

Teachers in general are not aware of or involved in any way with their students’ online activities.

Key Conclusion/Recommendations

The study points to the dire need of awareness and training sessions on cyber crimes, steps to protect oneself, and reporting and redressal mechanisms. Parents, caregivers and teachers have a crucial role to play in this regard. Institutions such as schools, colleges and even Child Care Institutions (CCIs) need to create safe spaces and peer groups through which children can support one another with information regarding prevention and redressal. Workshops and training should also be provided to law enforcement officials on effective investigative procedures. All stakeholders need to be sensitised to ensure their activities and attitudes are victim-centric and that shaming, blaming and guilt-tripping need to be avoided at all cost. Counselling services need to be provided to victims who come forward to report crimes, and redressal processes should be transparent, quick and effective. Finally, a collaboration of all stakeholders is required to effectively tackle cyber crimes against women and children.
What's Next?

This study has shown that cyber abuse and fraud are common among women and children in the districts under study. The recommendations made at the end of the study need to be addressed as a priority by all concerned stakeholders in order to ensure safe online experiences of women and children.

While this project adopted exploratory and descriptive research designs, the findings point to the need for large-scale studies on the topic that can inform interventions at scale. Future studies can focus on those who began using the internet in the aftermath of the pandemic, to understand new issues, challenges and trends with respect to online abuse in India. A study of those who have been using the internet for longer periods could focus on changes in their internet usage and experience over time.
Introduction to the Research Study

Scope of the Study

This study set out to explore online experiences of women and children in rural or semi-urban regions of India. Conversations around online safety and cyber crimes have assumed a level of significance in India (as around the world), especially as a result of the pandemic, owing to the increased exposure to internet services without any simultaneous capacity building and training. Incidentally, women and children began to get increasingly victimised in cyberspace, forcing some to even discontinue use of said services in the absence of any guidance on reporting or redressal. Additionally, issues of shame, stigma and victim-blaming lead women and children to cope with the emotional consequences of abuse, often without any external support or help, leading to long-term consequences. Despite these factors, not much effort has been directed towards specifically studying the experiences of women and children, especially of those in non-metropolitan areas of the country. Additionally, a lot of dialogue on cyber abuse and cyber crimes revolve around the issues of financial fraud and cyber bullying. Other forms of cyber abuse have not been given as much attention. In this context, it is crucial to note that cyber crimes are complex and multi-faceted, and there’s much more brimming beneath the surface than meets the eye. For example, Child Sexual Abuse Material (CSAM) floating online is linked to sexual exploitation of children and sometimes even trafficking. Again, some loan scams can result in trafficking towards repayment. In other words, exploitation begets exploitation and it is the need of the hour to nip such crimes in the bud. Unfortunately though, neither the consumers, nor key stakeholders are trained to handle such issues.

In this context, this study is an attempt to explore these aspects and provide perspective of women and children whose voices and experiences often do not come to the fore. The study does not intend to generalise its findings, but challenges the disproportionate interest in the online experiences of people in urban settings alone, which may be based on various assumptions or circumstances. Thus, this study set out to collect data on the online behaviour and experiences of individuals in rural and semi-urban areas cutting across crimes such as cyber bullying and stalking, impersonation and identity theft, phishing, cyber harassment and exposure to objectionable material. Additionally, study participants were
asked questions about their knowledge, perceptions and responses to cyber crimes and abuse.

We therefore aim to direct the spotlight on women and children in non-Tier 1 cities, with the hope that future interventions and solutions will include their experiences and provide holistic recommendations that benefit them as with those in urban locales.

It would be prudent to add here that this is not an exhaustive study of the problem in rural or semi-urban settings. While we may be only scratching the surface with this project, we point towards questions for future research projects on the topic.

Need and Purpose of the Study

Given the increase in cyber crimes against women and children, it becomes pertinent to understand, from a wider perspective, people’s experiences online and their responses to it. Firstly, despite dispersed newspaper reports on the topic, discussions on the overarching issue are few and far between and so are studies that seek to explore the issue from the perspective of women and children’s activities and experiences. Secondly, while discussions about cyber abuse have happened in a piecemeal fashion from urban locales such as Tier 1 cities, not much effort has gone into studying trends of online abuse that could be affecting women and children from rural regions where internet adoption and device usage has been increasing, especially as a result of the pandemic. Again, existing studies have tried to understand the perspective of children in schools, but what about those in the community who may or may not be in schools?

We want to address, at this juncture, that this study also set out to explore the hypothesis that lack of digital access for women and children in rural areas of India directly results in a lack of exposure to online abuse and crime. Not only is internet penetration extending to rural areas in a rampant and fast-paced manner, but additionally, women and children are accessing the internet despite their ownership of devices. So what really does the data suggest? How common is cyber abuse among women and children in rural and semi-urban India?

Again, in acknowledging that certain rural areas have traditionally been source and transit areas of human trafficking, it is important to study the penetration of perpetrators into online platforms in these areas for identification and victimisation of women and children. We
wanted to explore the use of technology and the internet towards trafficking in persons, through the experiences of young internet users in certain rural and semi-urban districts.

Several questions begged to be answered. How common are cybercrimes in rural and semi-urban areas? How are children and women being victimised online? What are their responses to them, if any? How open are people to talking about these issues? What are their perspectives and opinions on the topic?

### Research Design and Methodology

The research study followed a descriptive and exploratory design to understand the experiences of women and children with cyber abuse and fraud in rural districts of Jharkhand, Madhya Pradesh, Rajasthan and West Bengal. The field work was conducted through in-depth interviews covering aspects of cyber abuse experiences and responses.

Firstly, four states in India were chosen for the study- Jharkhand, Madhya Pradesh, Rajasthan and West Bengal. Although they don't represent states that have maximum reported incidences of cybercrimes against women and children, we had knowledge through partner NGOs that these states have been affected by cyber fraud and abuse. There are various reasons for underreporting of cybercrimes (as with other crimes involving abuse) and thus, reporting alone does not act as the primary indicator of actual incidence of abuse. Secondly, two districts each were chosen from the four states for the purpose of field work- Jaipur and Udaipur districts of Rajasthan, Bhopal and Raisen districts of Madhya Pradesh, Jalpaiguri and South 24 Parganas districts of West Bengal and Deoghar and Khunti districts of Jharkhand. The criteria for selection of districts included reportage of cyber abuse incidents in news reports, prevalence and high incidence of trafficking in persons. As the field work was conducted by partner NGOs and other CBOs, the final shortlist also took into account the presence of organisations working with women and children interested in this area of study in the chosen states.

Interview schedules were employed to conduct interviews with women and children ranging from the ages of 13 to 35 years. Since the study was exploratory in nature in that it sought to understand current and changing trends of online abuse and trafficking among women and children, the focus was on asking the participants about their online activities and experiences. Thus, the sample size was small- 108 per district. Out of that, 36 interviews
each were conducted with participants from the following age groups covering children, young adults and adults- 13-18 years, 19-25 years and finally, 26-35 years. Within each district, three locations were chosen for the field work by the concerned CBO/NGO following the given rationale- a third of the interviews were conducted in the city or town area or the district centre, another one-third were conducted in a block close to the district centre and one-third was conducted in a block further away from the city centre. It is important to note here that while these criteria were followed in most of the chosen districts, in certain cases, practical difficulties such as distance and a lack of resources (time and finances) influenced the choice of blocks for the study. We would like to add here that the sample for data collection was slightly different in the two districts of Madhya Pradesh. Here, only school children from one government school each of the two districts were interviewed. The sample size from these districts is also smaller than that of the other districts due to certain practical constraints. We would like to add that the school in Raisen district is a girls-only school while that from Bhopal follows a co-ed system. Additionally, a focus group discussion (FGD) was conducted with some teachers from the Raisen school on their experiences with cyber crimes and abuse while some teachers from the Bhopal school were interviewed on the same matters.

The data collection was done by teams using their smartphones through which they recorded responses via Google Forms. While the interview schedule was originally prepared in English, it was translated into Hindi and Bangla to ensure that the interviews could be conducted effectively and in a language convenient for both the interviewer and study participant (interviewee). The interviews took, on an average, about half an hour to complete. All the interviews were conducted with individuals who use the internet at least once a month, that is, with active internet users. The participants included school and college students, teachers, housewives, professionals and others. Prior to conducting the interviews, the participants were given a brief introduction to the topic of study and verbal consent of the participants was taken. In the case of the children from Bhopal and Raisen, the consent was taken from the Principals of the schools.

### Limitations of the Study

The study was conducted in a total of two districts each of Rajasthan, West Bengal, Madhya Pradesh and Jharkhand. While the study was planned, designed and coordinated by
Space2Grow in collaboration with CyberPeace Foundation, the field work was conducted in each of the districts by individuals or members of NGOs, that is, people based locally. Once organisations and individuals were contacted and data collection teams finalised, they underwent an online training session which covered the objectives of the study, interview schedule format and the sensitivities to be followed in the interview process. Post the training, all data collection teams were asked to submit mock forms prior to visiting the field in order to enable them to familiarise themselves with the interview schedule, topic and the process. While training was provided and the interview schedules (attached in the Appendix section) additionally came with detailed instructions and definitions of various cyber abuse for easy reference of the interviewer, one cannot rule out the possibility of errors in the interview and data capturing processes, given that the Space2Grow team could not be present to supervise the fieldwork.

Secondly, the nature of the study was such that it would not be possible to conduct field work with a representational sample. Instead, the focus was to conduct interviews with participants covering aspects such as internet use and user profile, experience with various forms of cyber abuse, responses to such abuse (if any) and knowledge and perception of participants about the issue at large. Thus, in-depth interviews were conducted with a small sample size from each district to understand their exposure to the internet, awareness and experiences of cyber abuse and fraud and responses to those.

With this introduction to the study, we shall now take a look at existing literature and data available on cyber crimes in the country, along with information on victimisation of women and children in online platforms. What have been the recent trends with respect to usage of the internet and mobile devices by women and children? What are the reasons for the spike in internet usage by people across genders, age groups and geographical locations and what have been the effects of said use? The following section will examine these questions and in doing so, anchor the subsequent section which details the study findings.
A Review of Literature on Online Abuse and Trafficking in India

Digital technologies and the internet are avenues providing immense opportunities for personal and professional growth, networking and self-expression. In the recent past, cyberspace began replacing physical spaces for hitherto routine offline activities in the context of the COVID 19 pandemic, with a large number of people starting to access the internet for work, learning, shopping, banking, entertainment, and social networking. This marked a fundamental change in the way people access and use internet facilities.

Recent reports reflect the increase in internet usage among people in India, particularly among women. According to the study report 'Bharat 2.0', in India there is a 61 per cent increase in the number of female active internet users, 24 per cent increase in the number of male active internet users, 45 per cent growth in the internet users from rural areas, and 28 per cent increase among the urban users since 2019 (Abrar, 2022). It also reports that India has 646 million active internet users aged two years and above as of December 2021. Among them, 592 million are aged 12 years and above with an increase of 37 per cent from 2019 (Abrar, 2022). These statistics reflect the magnitude of internet penetration in the everyday lives of people belonging to different age groups and gender across diverse geographical locations.

The report also states the utilisation pattern of internet facilities. Among the top five internet activities for the 12+ years age group, social networking and chatting are at the top, followed by video watching and listening to music (Abrar, 2022). For two-thirds of the youth in India,

---

1. Nielsen, a global leader in audience measurement, data and analytics conducted Bharat 2.0 Study which was designed to establish the Internet penetration and user profile for the country. The methodology is composed of face to face systematic stratified random surveys across all states and towns/villages. This was carried out from September 2021 to December 2021 covering ~110,000 household members across ~27,900 households.

social media is the medium to connect with family and friends, a medium of psycho-social support, information-sharing and entertainment (Mukherjee et al., 2021). India has the second largest user base of Facebook next to the US (Mehrotra, 2017). 54 per cent of the nearly 440 million internet users who watch videos are from rural areas (Abrar, 2022). Though 56 per cent of active internet users are in rural areas, online shopping and online banking facilities are mainly utilised by urban internet users (Abrar, 2022). The geographical differences in internet activities reflect varying digital skills and knowledge of users. Given that e-commerce and online banking require additional knowledge and skills, urban users who are relatively more educated and better employed have an edge over the internet users from rural areas, who rely on internet services mostly for entertainment and social networking purposes.

There is a reported gender difference among the proportion of male to female online banking users which stands at 69:31 (Abrar, 2022). Additionally, there is a stark gender divide in the social media space, as only 33 per cent women access social media against 67 per cent of men in 2019 (Mukherjee et al., 2021). Women have relatively less access to electronic gadgets such as smartphones and computers with internet facilities. This acts as a barrier for them to access resources and knowledge that can aid their empowerment.

The rise in the number of active internet users among women and children above 12 years is an encouraging sign of growth in digital literacy. Though there exists a gender divide, social media has played a significant role in enhancing the professional and personal lives of many women, particularly during the pandemic. It provided economic opportunities for women through new jobs, avenues of networking and collaboration for women entrepreneurs to establish and expand their marketing, along with professional skill development and capacity building (Sattva, 2021). For many women, social media sites allow for self-expression, act as spaces to connect with family and friends and network with interest groups to support social causes, thus boosting their social and emotional well-being (Sattva, 2021).

In recent times internet services have been increasingly adopted by children as well. According to the estimates of UNICEF (2016) one third of the internet users across the globe are children; the International Telecommunication Union (ITU) statistics in 2017 states youth (15-24 years) are at the forefront of internet adoption (Sattva, 2021). The pandemic contributed to increased access to digital devices among children with physical classes getting replaced by online platforms of learning. Students mainly access the internet for online search of information, tutorials, group discussions among peer groups, and to
connect to their formal school education programmes (CRY, 2020). They also access the internet for entertainment purposes, such as gaming, watching videos and social media.

Though the internet provides immense opportunities, cyber security is largely compromised with the increase in cybercrimes and online abuse. Cyber violence and online trafficking of women and children is a growing concern as more and more women and children are accessing cyberspace since the beginning of the pandemic.

Cyber Security Risks of Children in Virtual Learning Spaces and Gaming Portals

The unprecedented growth of EdTech companies over the last two years or so in the absence of a clear regulatory framework, especially on questions related to pricing, advertising, curriculum and digital safety, has been a major concern for governments as well as civil society organisations (“Government warns,” 2022). Online learning accelerated the growth of EdTech companies to 1.96 billion USD digital education market in 2021 from 0.247 billion USD business in 2016 (Reddy, 2021) as schools and non-governmental organisations also utilised their services to reach their students during the school closures in the pandemic. Despite their role in enabling continued learning for children during school closures, EdTech platforms inadvertently became spaces where students became victimised through different forms of abuse or issues related to privacy.
This growth of EdTech companies and weak data security protocols raises data privacy concerns for children. Human Rights Watch, an international organisation, reported that 164 education apps and websites run by both private entities and governments across 49 countries including India are susceptible to deficient services that risk children's privacy, confidentiality and safety (Aryan, 2022). In the Indian context, particularly in rural areas, the lack of awareness of parents about cyber risks, due to poor digital literacy and low education levels has a serious bearing on the safety of children (Reddy, 2021). Additionally, in the absence of regulatory policies and guidelines to protect privacy, children are vulnerable to sexual offences. The visual presentations and live video or conference calls during online classes, and learning activities involving videography are shared in virtual spaces, running the risk of sexual predators accessing these images and videos, and the location of the child (Krishna & Sharma, 2021).

Another area of online engagement for children that poses threats while having many advantages is that of gaming. Firstly, what is online gaming? It refers to video games that allow and require interactions with other players. The two things one needs to be careful of are the amount of information that players share with each other and the number of people they interact with in the course of a game. While online gaming platforms offer its users avenues for fun, teamwork, collaboration, imaginative adventure etc., it carries with it some significant risks, especially for children. The risk of online gaming addiction, for one, is quite real as the completion of each level releases dopamine, a potent neurotransmitter, that plays a role in how one feels pleasure. Gaming platforms bring its players in contact with strangers and there is now reportedly an overlap between gaming and social networking. In fact, children's first online interaction with a stranger is now more likely in a video game. This has made online gaming one of the preferred platforms for online groomers who interact and get friendly with children or those much younger than them with an intention of sexual abuse. In these games, players do not necessarily know who they are playing with and thus it is easy for online predators to remain masked while carrying on their activities. Other issues with online gaming include rampant cyber bullying of a player by other players, which could extend to offline abuse, loss of privacy and exposure of personal information, hacking, malware, hidden fees and in-app purchases that can push children to steal their parents' money or use their credit/debit cards without permission to purchase new features or to access new levels of a game.
Hence, there is a need to consider the changes brought on by these platforms with respect to children’s safety, privacy and other risks and to take steps to ensure that children are able to take advantage of these while steering clear of abuse and addiction.

**Cyber Violence Against Women and Children**

Though internet facilities act as enablers for women and children, the accompanying cyber violence against them is a cause of concern. As women and children began increasingly accessing the internet and digital devices, they also began getting increasingly victimised online, as we shall see. Cyber violence is identified as a form of gender-based violence that has social and economic consequences (EIGE, n.d.). Cyber violence against women is the outward expression of existing misogyny and gender inequalities in society and is a continuum of violence in physical spaces (EIGE, n.d.). Recent incidents of TikTok videos glorifying rapes and acid attack, incidents of trolling, bullying, increase in harassment of women on social media sites escalate women's risk of violence and highlight their lack of digital safety. The National Commission of Women also reported an increase in reporting of online cybercrime complaints in 2020 compared to 2019 (Mukherjee et al., 2021). According to Statista, a German company specialising in market and consumer data, 18,066 men were arrested in cyber crime cases in India as against 354 women, and 17,721 men were charged with legal proceedings for cyber crime cases compared to 468 women, in 2020. This points to the disproportionate involvement of men in cyber offences as against women perpetrators.

The common types of online harassment include cyber harassment, cyberstalking and cyberbullying. Cyber harassment is intended to offend or hurt a person online through threats of violence, sexually explicit messages, or hate speech intending to terrify, humiliate or harass, and intimidate their victims. It commonly occurs on social networking sites, emails and chat rooms. Cyberstalking poses a threat of harm to the victims. Here the victims receive repeated messages or emails in an unwanted manner, or perpetrators access or hack their social media account to track their online activities, comment on their online posts unnecessarily, and steal their personal information with the intention to cause harm. In many cases, cyber stalking and cyber harassment are a prelude to inflicting physical violence and harassment upon the victims.

Cyberbullying is a rampant form of cybercrime by an individual or a group through deliberate and repeated hostile acts that cause harm to the dignity and reputation of their victims. This
includes sexually explicit remarks, threats of violence or sexual harassment, defamatory accusations, online denigration of the targets through posting rumours about them, hacking into their social media accounts and posting comments intended to humiliate them. The #MeToo movement in the recent past reported many such cases of cyberbullying on public platforms (Chugh, 2018). Recent examples of cyberbullying of women include the targeted attack of over 100 women journalists, social activists and active users of social media through the fake online auctioning site 'Bulli Bai' and, 'Sulli deals’ an app hosted by GitHub (the web-based open source application). This online sexual violence centred on the religious and gender identities of its victims and was intended to humiliate and silence outspoken women (“Bulli Bai case”, 2022).

The online games of Blue Whale and Momo that sets as a challenge for users to take their own life is another case of cyberbullying of children from recent times. Children often become victims of online bullying and harassment in online classrooms by their classmates, peers and sometimes even by teachers. Unregulated platforms with weak safeguarding policies and a lack of clear definitions of appropriate cyber conduct add to the risk of the vulnerability of children on online platforms.

Women activists, journalists, and outspoken women from minority religious and ethnic communities active in cyberspace have widely been attacked with cyberbullying, cyberstalking, sexist abuse, defamation, threats of sexual violence, morphing, hacking, and publication and circulation of online sexual abuse materials. Social media platforms such as Twitter have become sites of toxic trolling and cyberbullying while Facebook has been used to harass women through identity theft and morphing (Mukherjee et al., 2021). While it might seem like only women in the limelight are targeted online, this is far from the truth. In fact,
given the underreporting of online abuse and taboos around victimhood, stories of women often do not get known or reported.

Cyber grooming has been widely used by perpetrators to befriend, groom and gain the trust of their targets in cyberspace, particularly women and children, for sexual exploitation. Social networking sites are often used as a medium for cyber grooming by sending friend requests to targets and gradually befriending those who respond to their messages. Certain reports state that human traffickers are widely using cyber grooming techniques to traffic their victims into the sex trade.

The increase in online platforms offering various sexual services has altered the nature of child trafficking (Keishing, 2021). According to the National Crime Records Bureau (NCRB) data, 2,914 child trafficking cases were reported in 2019 (NCRB, 2020). NCRB further also found that there is a 400 per cent increase in cybercrimes against children in 2020 compared to 2019. Most of these are related to publishing or transmitting materials depicting children in a sexually explicit act (“400% increase in cybercrime”, 2021). During the pandemic-induced closure of schools, children accessed the internet to attend online classes and for learning purposes without much supervision from parents; along with this, the increased dependence on the internet for entertainment purposes during lockdown made children vulnerable to sexual exploitation. Commercial Sexual Exploitation of Children (CSEC) which includes child sexual abuse material (CSAM), cross-border sex trafficking, and child sexual exploitation through internet websites and social media also worsened during the pandemic.

Interpol reports say India is at high risk on the target list of online stalkers and paedophiles (Bose, 2021). Global NGOs acting as internet watchdogs alerted the need to protect children as there is an increase in demand for CSAM on the dark net and paid porn sites (Bose, 2021), particularly during the pandemic lockdown period (Munshi, 2020).

The National Centre for Missing and Exploited Children, the US-based NGO shared over 25,000 Tipline reports on CSAM materials suspected to be uploaded on social media in India (Babu, 2021). Cyber police investigation revealed incidents of using malware for tapping the webcam of victims to steal information or take pictures (Babu, 2021).
According to NCRB data, there is an 11.8 per cent increase in reported cybercrimes in 2020 of which 60.2 per cent involve cases of fraud, while 6.6 per cent involve sexual exploitation (“India reported an 11.8% rise in cybercrime”, 2021). Reports indicate a significant increase in reported cybercrimes in India during the pandemic-induced nationwide lockdown period from March to August 2020, as routine activities such as work, shopping, and social gatherings moved to virtual spaces. In Delhi alone, a maximum of 4000 cases were reported for each month from May and August 2020. Out of these, 62 per cent were of crimes of financial fraud while 24 per cent involved social media harassment (Mukherjee et al., 2021).

Financial fraudsters make use of technology and exploit various online platforms including e-banking, social media profiles and online marketing sites. They operate in multiple ways such as creating fake online shopping portals, distress calls for help using fake social media profiles, sending phishing links to mobile phones and email accounts, making scam calls with fake SIM cards, sending messages offering jobs, offering cashback and other freebies, sending SMS leading to scratch card portals etc. to dupe people (Haider & Upadhyay, 2021). Bharatpur, Mathura and Mewat which constitute the tri-junction of Rajasthan, Uttar Pradesh and Haryana have been reported as the new 'Jamtara', Jharkhand's shady town infamously known as the hotbed of financial fraudsters (Haider & Upadhyay, 2021).

Recent reports project that small towns and rural areas are not immune to cybercrimes. It is, in fact, of alarming concern as there is a growth in the number of active internet users in rural India. The economic growth of Tier II cities, easy availability and affordability of digital devices and low internet data cost, contribute to an increase in the number of internet users in these cities. The quarterly report, 'Q2 findings of Cyber Threat Monitor (CTM)' reported the vulnerability of Tier II cities to cyber security threats, with Patna (47 per cent), Guwahati (45 per cent), Lucknow (44 per cent), Bhubaneswar (43 per cent) and Jaipur (40 per cent) depicted as susceptible to cyber attacks (“Indian Tier-II cities”, 2019). It also reported that three in ten netizens in India have encountered cyber attacks in these cities (“Indian Tier-II cities", 2019).

Jharkhand’s Jamtara is known as the cybercrime capital of India (“This town in Jharkhand", 2018). The extremist insurgencies, crimes against women and cybercrimes are major challenges faced by the state law enforcement authorities. In the first 11 months of 2021, 919
cases were reported in the state (Sahay, 2021). The recent reports show a spread of cybercrimes from Jamtara to the adjacent district of Deoghar. Police report that cyber criminals from these small towns operate in a similar fashion as that of IT companies, and that mainly teenagers are recruited and trained to become professional scammers. The reports of the involvement of teenagers and children expose the vulnerability of children to cybercrimes ("Jharkhand's cybercriminals", 2020). With the pandemic and lockdown, a large number of migrant labourers returned to their hometown in light of the loss of employment at their places of work. In this scenario, easy money through cyber fraud lures people to cybercrimes. There are reports of family members joining their relatives already involved in cyber frauds during the pandemic ("Jharkhand's cybercriminals", 2020).

Jharkhand also witnesses high rates of crimes against women and children. Human trafficking of young children and women in Jharkhand for the sex trade and forced labour are a concern for the government and civil society organisations ("Kailash Satyarti NGO ‘rescues”, 2022). The pandemic has also resulted in worsened structural inequalities with loss of employment and an increase in poverty. This has escalated the vulnerability of children and women from marginal communities, particularly Dalit and Adivasi communities, and impoverished families to trafficking and exploitation (Keishing, 2021).

Cybercrimes such as online stalking, and online sexual harassment of women are also increasing in recent times. In this context, the state government has collaborated with the nationwide cyber awareness campaign initiated by the National Commission for Women 'Digital Shakti Campaign' in 2019 (Bose, 2019). This campaign is a joint initiative of the National Commission for Women in association with Facebook and CyberPeace Foundation to promote digital literacy among women and girls, creating awareness of the prevalence of cyber threats and available redressal mechanisms for women through training and capacity building (Bose, 2019). In December 2021, NCW and the Jharkhand government jointly launched an online resource centre for cyber safety of women collaborating with the above stakeholders. They also launched a WhatsApp helpline number for women to reach out in case of distress and to provide assistance in case of cyberbullying, cyberstalking and other forms of cyber violence.

West Bengal is the epicentre of India’s human trafficking, particularly child trafficking for sex trade ("West Bengal", 2020). According to NCRB reports, West Bengal is one among the states that report the highest number of missing women and children annually, with 8000 children reported missing in the period 2016-2018. Poverty and poor education force young
children to work in factories and small shops to earn for their families. Young girls and women from these vulnerable families often fall prey to trafficking. The targets of child trafficking include children from the upper middle class and broken homes as well. They are often lured by boyfriends, strangers or at times even by family members with a promise of a better future, misled by romance, the promise of marriage and employment opportunities (Mazumdar, 2020). Most of them are sold to brothels or domestic labour (Mazumdar, 2020). During the pandemic, cyberspaces became growing sites of exploitation by traffickers. Social media platforms such as WhatsApp and Facebook are manipulated by the perpetrators to build contact with and groom targets (Mazumdar, 2020).

In Kolkata, young teenagers from classes IX to XII were trained to start campaigns against trafficking and human rights violations as trafficking began penetrating online spaces (Mazumdar, 2020). International organisations working in the area of anti-human trafficking initiated capacity building in young children, as traffickers increasingly began to trap young students and children online to solicit sexual services for their clients. Young children are befriended on online platforms by perpetrators with false identities to collect private information and seek salacious videos and photographs, later used for blackmailing the victims. There are also reported instances where the victims were asked to join private online groups and perform sexual acts. The perpetrators also send the links of these sexual abusive content to their clients for money (Mazumdar, 2020).

In West Bengal, the pandemic and the cyclone Amphan landed major blows to the safety and security of women and children as they escalated the multidimensional poverty and forced labour migration. The Calcutta High Court had given direction to the West Bengal
government to ensure adequate measures for the protection of children during the pandemic anticipating an increase in trafficking. The move of the High Court in this regard was in the light of the report submitted by the West Bengal Commission for Protection of Child Rights (WBCPCR) that provided data to the High Court on cases of child marriage, child trafficking, child sexual abuse and violations of child rights (Das Gupta, 2020).

Crimes against women are a growing concern in Madhya Pradesh. Based on the reported offenses against women in the state in 2017 and 2016, Madhya Pradesh was termed as the rape capital of the country. A total 5,562 cases of rape, including that against minors, were registered in the state in 2017. In the same year, the state also topped the chart with highest percentage of reported cases of domestic violence in the country—39 per cent of all reported cases ("Domestic violence against women", 2019). National Crime Records Bureau reported 30,813 cases of abduction, sexual assault, eve teasing and human trafficking of women and children in 2021. Kidnapping is an additional grave concern in the state. During the pandemic years 2020 and 2021, over 17,716 people were abducted, of which 7,733 are still to be traced. Women and children constitute a large proportion of the victims of abduction. A total of 7,856 minors and women, and 2,117 boys and men were abducted in 2021. Of these, the number of minors abducted during this period is 7565 girls and 2016 boys ("Bhopal: 1,341 women were abducted for marriage", 2022).

The safety of children in Madhya Pradesh is at stake with more than 17,000 crimes against children, which is the highest in the country in 2020 ("Madhya Pradesh becomes most unsafe", 2021). Sexual assault on children is also rising with 3,522 reported cases under the POCSO Act and IPC Sec 376 (rape) in the year 2021 ("Bhopal: 1,341 women were abducted for marriage", 2022). Cyber crimes against women and children are also rising though they are under reported. Cases of child sexual abuse material (CSAM), cyber bullying, morphing, transmission of pornography were reported in the state in 2021. Bhopal district saw a massive increase in reported cyber crimes, with 1,800 cases reported between January 1 to May 25, 2022, which is more than double the cases reported in the year 2021. There is a steady increase in cases reported post-pandemic, with over 12 cases being reported per day in Bhopal city. A large share of the cases reported are of financial fraud (Mishra, 2022). The first two months of 2022 reported a 32 percent increase in the cyber crimes against women in Bhopal which includes sextortion, transmission of morphed pictures in social media, sexually explicit comments and creating fake social media accounts (Mishra, 2022).
Though authorities have launched widespread campaigns and issued advisories to create awareness among people on cyber crimes, the inadequacy of police stations to address them is a matter of concern (Mishra, 2022). In the backdrop of rising cyber crimes against women, Harda district administration in MP has launched *cyber sakhis*¹ to fight cyber criminals and train women and girls to educate others on matters of digital safety, particularly the women in the rural areas (Ranjan, 2022). Madhya Pradesh Commission for Protection of Child Rights (MPCPCR) also organised a workshop for master trainers on Right to Education, Child Safety, Mental Health of Children and Cyber Crime (“Madhya Pradesh minister stresses”, 2022).

CSAM is a growing concern in Rajasthan along with an increase in reported rape cases (a total of 5,877 cases were reported up until November in the year 2021) (“Rajasthan: Rape cases”, 2021) and child trafficking (815 in 2020). The reports show that there was a rise in crimes in Rajasthan during the pandemic even when most states in India had a decline in overall crime rates. Child marriages and violence against women are a growing menace in Rajasthan. Recently the US-based organisation, The National Centre for Missing and Exploited Children has shared information on 22,000 incidents of CSAM with the state officials in Rajasthan (“5,000 Child pornography cases”, 2021). The probe on some of the above cases led to the arrest of some people in Jaipur who accessed CSAM contents (“5,000 Child pornography cases”, 2021). Other news reports also show that Bharatpur and Jaipur regions are growing hotbeds of cybercrimes in Rajasthan.

The absence of forensic and cybercrime experts in solving cybercrimes is a major challenge to the Rajasthan law enforcement authorities. It leads to the piling up of cases in many districts given the surge in reported cases (“cases pile up”, 2021). Mismatch of the jurisdiction of police stations under the complaint lodged, and lack of cooperation from victims during the probe of the case are other hindrances to resolving cybercrimes for state officials (“cases pile up”, 2021).

---

¹ *Cyber sakhis* are anganwadi workers and community volunteers trained as master trainers to educate women on matters of digital safety and to confront cyber criminals.
Challenges in Combating Cyber Crimes

The experts opine that cybercrimes in India are “massively under-reported” and the statistics of reported cybercrimes do not capture the ground reality (Das, 2017). The major challenge in combating cyber violence is people's lack of knowledge and understanding of various types of cybercrimes and threats to their cyber security. There are reports that netizens, particularly youngsters, are lenient in adopting digital safety measures.

Socio-cultural factors act as barriers to reporting cybercrimes. Cyber violence, although meted out via virtual platforms, always results in tangible effects for the victims. Yet, the fear of causing dishonour, social stigmatisation and taboo discourage many victims from reporting crimes. Lack of awareness of law enforcement agencies in dealing with cyber crimes leads to a lack of seriousness on their part to investigating them; this acts as a barrier in reporting as victims feel it's an unnecessary hassle trying to seek justice. This in turn encourages the perpetrators to become ‘reckless experts’ in cybercrimes such as morphing, and hacking by evading law enforcement agencies (Borwankar, 2022).

Perpetrators thrive on their anonymity in cyberspace. There are reports of cyber criminals increasingly using the dark web, an encrypted part of the internet that cannot be easily tracked, for carrying out their criminal activities. There is also easy availability of tools required for cyber crimes on the dark web. The lack of access to the dark web by standard search engines complicates the scenario, as it requires specific information about the criminal activity and special training for the police officers to track cyber crimes committed using the dark web (Kaushik, 2019). The structural and functional incapacities of the law enforcement authorities such as inadequacies of expertise and capacities of police, insufficiency of cyber cells and lack of properly equipped cyber forensic laboratories are major challenges in combating cybercrimes (Borwankar, 2022).
The involvement of international gangs makes the case more complicated as they successfully avoid detection by law enforcement agencies as the servers used are located outside national boundaries. Bilateral treaties, international cooperation and cyber policies addressing these loopholes are required to combat the crimes in these situations. However, the registration of criminal cases is the primary step in tracing, arresting and prosecuting criminals located outside India (Borwankar, 2022).

Roundup of the Literature Review

The pandemic marked a significant phase in terms of changing trends in usage of internet services by people around the globe. Virtual spaces replacing (at least partially) physical spaces for routine activities continue even in the post-pandemic phase with many people still working from home, depending on online shopping facilities, online banking and digital payment services, students accessing online learning platforms provided by EdTech companies, accessing online entertainment contents and online games. Easy access and affordability of digital devices and mobile data facilities have revolutionised internet accessibility patterns with an increase in internet users from rural areas and small towns in India. Most internet services make daily life easier and more convenient for the users. Though
digital empowerment is a positive sign of development, it also raises serious concerns about
digital safety.

The rise in cybercrimes during the pandemic when there was an overall decline in reported
crime rates indicates the increase in vulnerability and risk of users to cyber crimes with an
increase in the number of internet users in different age groups and gender across different
geographical locations. In the Indian context, poor education and digital literacy of the users,
particularly in the rural areas and small towns, add to the vulnerability of the users to cyber
criimes. Their lack of awareness of cybercrimes, and that of available redressal mechanisms,
often leads to underreporting of crimes and self-censoring by quitting the use of certain
internet facilities. Data tracked through cookies in websites on the usage patterns, interests
and preferences of users are used by content developers to develop their marketing
techniques to make profits by catering to the interest of their users. This, to a great extent, is
an infringement on the privacy of the users. Interventions are needed for capacity building of
internet users across different geographical locations and age groups, addressing
awareness building, digital safety measures and reporting of cybercrimes.

Given increased exposure of women and children to internet technology in recent times,
there is a need to focus on protecting them from the various dangers on the internet. With
increased internet usage, the study participants also began facing abuse and fraud online
but as we will see, official reporting of the same is abysmally low. Part of the reason is that
there are almost no conversations around digital safety, forcing women and children to turn
to friends and peers to talk about their online experiences. These friends are equally
ill-equipped to deal with such issues and can do precious little to help their defrauded
friends, other than in lending an empathetic and listening ear. There needs to be a
momentous shift in these attitudes in order to ensure that women and children are able to
benefit from the resources and opportunities presented by the internet and that their
vulnerability on these mediums are parallely reduced.

In the following section, we will study the findings of this research initiative, pointing to
issues and responses by study participants to their online experiences. Following this, we will
also consider possible solutions that can be undertaken to address these issues.
Trends in Online Abuse and Trafficking of Women and Children: Study Findings

As mentioned in earlier, the field study for this report was conducted in four states, viz. Rajasthan, Jharkhand, Madhya Pradesh and West Bengal. The choice of states for the study was done basis the high incidence of human trafficking (given these states serve as source and/or transit hubs for trafficking in persons), increased adoption of mobile and internet technologies, along with available data on cyber crimes. Apart from these reasons, another significant source of information is Space2Grow’s partner organisations located in these states that shared their experiences with handling cyber crime related issues on behalf of the communities they work in. From each state, two districts each were chosen for the field study. These were Khunti and Deoghar (Jharkhand), Jaipur and Udaipur (Rajasthan), Bhopal and Raisen (Madhya Pradesh) and Jalpaiguri and South 24 Parganas (West Bengal).

This section of the report examines the results and findings from the field survey conducted in the districts mentioned above. Let us now delve into the responses of women and children surveyed and through it explore the existing trends in online abuse in the given locales.

Profile of the study participants

The sample size for the field survey was 108 participants per district (except in MP where the sample size was about half that number), who were divided into three age categories of 36 participants each- 13-18 years, 19-25 years and 26-35 years. However, given the fact that data collection team members were deployed in different blocks and areas for the field study, the numbers don’t exactly match up in all districts, although they are in the ballpark of the intended sample size. Let us now look into the study findings.

The study has a total number of 749 participants, out of which, 316 lie in the 13-18 age group, 207 in the 19-25 years age group and finally, 226 in the 26-35 years age group. This is represented in the table below:
As the study was an exploration into the experience of abuse among women and children, girls and women formed a majority of the study participants. For the study, 165 boys were interviewed while the number of girls and women cumulatively added up to 584, or ~78 percent of the study participants.

Of the 749 participants, about 60 percent are single, 38.18 percent are married and about 1.60 percent are separated, divorced or widowed. The occupation of the study participants is represented by the following table:

<table>
<thead>
<tr>
<th>Occupation of study participants</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homemaker</td>
<td>186</td>
</tr>
<tr>
<td>School student</td>
<td>241</td>
</tr>
<tr>
<td>College student</td>
<td>127</td>
</tr>
<tr>
<td>Working professional</td>
<td>126</td>
</tr>
<tr>
<td>Unemployed</td>
<td>31</td>
</tr>
<tr>
<td>School dropout</td>
<td>37</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>749</td>
</tr>
</tbody>
</table>

### Table 2: Number of study participants according to occupation
With respect to educational qualification, most participants have some amount of education. About 18 percent are graduates and about four percent holding post graduate degrees. Just about three percent are illiterate or uneducated and 5.61 percent are school dropouts.

Data on internet usage

All the study participants are active users of the internet, i.e. they use the internet at least once a month. In fact, an overwhelming majority of the participants, i.e. 92.26 percent said that they use the internet daily, while 5.34 percent said they use it about two to three times a week. Out of the 316 participants who fall under the age group of 18 years and below, 286 (90.50%) said that they use the internet on a daily basis. Among those who shared that they use the internet daily, the following table represents the amount of time they spend on it per day. It must be noted here that out of the 691 participants who use the internet daily, only 630 responded to the follow-up question on how much time they spend online on a daily basis.

<table>
<thead>
<tr>
<th>Time spent online daily</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 hour</td>
<td>136</td>
<td>21.59%</td>
</tr>
<tr>
<td>1-2 hours</td>
<td>201</td>
<td>31.90%</td>
</tr>
<tr>
<td>3-5 hours</td>
<td>186</td>
<td>29.52%</td>
</tr>
<tr>
<td>Over 5 hours</td>
<td>107</td>
<td>16.98%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>630</strong></td>
<td><strong>100.00%</strong></td>
</tr>
</tbody>
</table>

Table 3: Hours spent online on a daily basis by participants who use the internet daily

Again, most of the study participants are those who began using the internet over the last five years. To be precise, 44.06 percent said that they have been using the internet for the last one to two years, indicating that they began using the internet after the outbreak of Covid. Among those who began using the internet over the past couple of years, most have predominantly used it for entertainment, social media etc. Some made use of it for school
and college related and professional work as well. 42.99 percent of all participants have been internet users for the last three to five years. This is represented in the table below:

<table>
<thead>
<tr>
<th>Duration of internet usage (in years)</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2 years</td>
<td>44.06%</td>
</tr>
<tr>
<td>3-5 years</td>
<td>42.99%</td>
</tr>
<tr>
<td>6-10 years</td>
<td>8.54%</td>
</tr>
<tr>
<td>Over 10 years</td>
<td>4.41%</td>
</tr>
</tbody>
</table>

Table 4: Duration (in years) of internet usage of study participants

The study also sought to find the type of device used by the participants to surf the internet. They were provided with the options of mobile phones, laptops or PCs, tablets and the use of public computers at cyber cafes. Study participants were allowed to choose multiple responses, recognising the fact that people may often use multiple devices to surf the internet. The study found that over 98 percent of the participants use mobile phones while 15.22 percent use laptops or PCs, 6.54% use tablets and 3.34% use public computers. Of these, 88.52% participants shared that at least one of the devices they use belong to them while 11.48% do not own any device. Again, about 98% shared that they predominantly surf the internet at home. Some others go online via personal devices in public places or while on the go amounting to about 39%, and finally, about 36% said that they use the internet at their workplaces or educational institutions.

People use the internet for various purposes ranging from work to entertainment and e-commerce, among many others. While this is true of any internet user, the study finds that among its participants, the predominant use of the internet is for entertainment, followed by social media. It needs to be noted that the percentage points in the column on the right do not add up to 100% since participants were allowed to choose multiple responses here. This is depicted in the table given below.
Clearly, social media is quite popular among the study sample: 94.66% of the participants shared that they use social media, of which about 87% said that they use Facebook, 59.60% use Instagram and 17.07% hold accounts on Twitter. Among the 316 13-18 year-olds who were interviewed for the study, 289 use social media. In other words only 3.60 percent of the children interviewed do not have an account on any social media. Two observations are thrown up by this data- we see that not only is social media popular among children but despite the storehouse of information and study material available online, children mainly use the internet for entertainment purposes.

Experience of cyber fraud and abuse among study participants

We shall now take a look at the experiences of cyber fraud and abuse as shared by the study participants. Where relevant, we shall consider comparative data of the districts under study. To begin with, the following table shows comparative data on time spent online by participants from the eight districts on a daily basis. This only takes into account those who have responded affirmatively to spending time online daily.
Almost 50% participants from Jalpaiguri who use the internet daily shared that they spend about 3-5 hours online. From South 24 Parganas we can see that almost 48% spend 1-2 hours online and about 37% spend 3-5 hours online on a daily basis. A majority of participants from Deoghar spend up to five hours online on a daily basis. Most participants from Bhopal and Raisen districts spend up to two hours online on a daily basis.

Since social media is a big component of the participants’ internet usage, we asked them about their activities and experiences on such sites. About 88% of participants shared that they have at some point, or do (in a continued manner) receive friend requests from unknown people on these sites. When asked about how they respond to such requests, about 11% shared that they read the profile of the concerned person and accept the request if they feel like it. 15.61% shared that they always accept friend requests, even from unknown people. Almost 32% shared that they accept such requests if they have common friends with the said person and about 42% shared that they always ignore or reject such requests.

While we have seen the overall trend with respect to response to friend requests from unknown persons via social media, the following table represents the district-wise information on how the participants respond to the same. The table shows that participants from South 24 Parganas district seemed to be highly risk-taking in this regard in always accepting such requests, followed by those from Khunti. At the same time, those from Jaipur

<table>
<thead>
<tr>
<th>Time spent online daily</th>
<th>Jalpaiguri</th>
<th>S 24 Parganas</th>
<th>Khunti</th>
<th>Udaipur</th>
<th>Jaipur</th>
<th>Deoghar</th>
<th>Bhopal</th>
<th>Raisen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 hour</td>
<td>0.93%</td>
<td>10.96%</td>
<td>16.49%</td>
<td>26.04%</td>
<td>14.17%</td>
<td>33.66%</td>
<td>34.62%</td>
<td>36.17%</td>
</tr>
<tr>
<td>1-2 hours</td>
<td>26.85%</td>
<td>47.95%</td>
<td>43.30%</td>
<td>37.50%</td>
<td>24.17%</td>
<td>29.70%</td>
<td>36.54%</td>
<td>51.06%</td>
</tr>
<tr>
<td>3-5 hours</td>
<td>48.15%</td>
<td>36.99%</td>
<td>31.96%</td>
<td>21.88%</td>
<td>20.00%</td>
<td>30.69%</td>
<td>7.69%</td>
<td>2.13%</td>
</tr>
<tr>
<td>Over 5 hours</td>
<td>24.07%</td>
<td>4.11%</td>
<td>8.25%</td>
<td>14.58%</td>
<td>41.67%</td>
<td>5.94%</td>
<td>21.15%</td>
<td>10.64%</td>
</tr>
</tbody>
</table>

Table 6: Time spent online daily by participants: District-wise data

Changing Trends in Online Abuse and Trafficking of Women and Children
seem to exercise much caution in this area by always ignoring or rejecting requests from strangers.

<table>
<thead>
<tr>
<th>Response to friend requests from unknown persons</th>
<th>Jalpaiguri</th>
<th>S 24 Parganas</th>
<th>Khunti</th>
<th>Udaipur</th>
<th>Jaipur</th>
<th>Deoghar</th>
<th>Bhopal</th>
<th>Raisen</th>
</tr>
</thead>
<tbody>
<tr>
<td>I always accept those requests</td>
<td>6.80%</td>
<td>46.91%</td>
<td>28.87%</td>
<td>10.13%</td>
<td>1.92%</td>
<td>5.83%</td>
<td>28.21%</td>
<td>2.44%</td>
</tr>
<tr>
<td>I always ignore/reject them</td>
<td>15.53%</td>
<td>23.46%</td>
<td>20.62%</td>
<td>39.24%</td>
<td>75.0%</td>
<td>55.34%</td>
<td>53.85%</td>
<td>65.85%</td>
</tr>
<tr>
<td>I accept the request if I have common friends with the person</td>
<td>43.69%</td>
<td>13.58%</td>
<td>42.27%</td>
<td>49.37%</td>
<td>22.12%</td>
<td>37.86%</td>
<td>7.69%</td>
<td>7.32%</td>
</tr>
<tr>
<td>I read the profile even if I don’t know the person and then accept if I feel like it</td>
<td>33.98%</td>
<td>16.05%</td>
<td>8.25%</td>
<td>1.27%</td>
<td>0.96%</td>
<td>0.97%</td>
<td>10.26%</td>
<td>24.39%</td>
</tr>
</tbody>
</table>

Table 7: District-wise response to friend requests from unknown persons

Receiving personal messages from unknown persons via SMS/Whatsapp/Messenger etc. is quite common. 85.31% participants shared that they have, at some point, received a personal message online from an unknown person. On being asked how they responded to said message, 33.12% shared that they read the message and responded appropriately, 34.87% said that they ignored the message, 19.11% shared that they blocked the sender and about 11% shared that they ignored the message after reading it.

Again, let’s consider the district-wise response of participants to personal messages received via online mediums. Participants from Deoghar, Jaipur and Khunti districts (followed by those from Udaipur), shared that they ignored the personal message shared while those from Jalpaiguri and South 24 Parganas displayed much risk-taking in that they decided to respond to the message received. The 8.74% responses from Khunti that came under ‘Other’ refers to the participants who said that they read the message and tried to find out who the
sender was. 80 per cent of the participants from Raisen shared that they blocked the sender while 25% of those from Bhopal responded appropriately while the rest ignored or blocked the sender and the message.

<table>
<thead>
<tr>
<th>Response to personal messages from unknown people</th>
<th>Jalpaiguri</th>
<th>S 24 Parganas</th>
<th>Khu-nati</th>
<th>Udaipur</th>
<th>Jaipur</th>
<th>Deoghar</th>
<th>Bhopal</th>
<th>Raisen</th>
</tr>
</thead>
<tbody>
<tr>
<td>I read the message and responded appropriately</td>
<td>55.10%</td>
<td>52.56%</td>
<td>27.18%</td>
<td>29.17%</td>
<td>12.5%</td>
<td>36.6%</td>
<td>25.0%</td>
<td>12.5%</td>
</tr>
<tr>
<td>I read the message and ignored it/did not respond</td>
<td>39.80%</td>
<td>17.95%</td>
<td>1.94%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>37.5%</td>
<td>5.00%</td>
</tr>
<tr>
<td>I ignored the message/ did not read it</td>
<td>0.00%</td>
<td>23.08%</td>
<td>50.49%</td>
<td>41.67%</td>
<td>52.08%</td>
<td>60.4%</td>
<td>17.50%</td>
<td>2.50%</td>
</tr>
<tr>
<td>I blocked the person</td>
<td>5.10%</td>
<td>6.41%</td>
<td>11.65%</td>
<td>29.17%</td>
<td>35.42%</td>
<td>2.97%</td>
<td>20.00%</td>
<td>80.00%</td>
</tr>
<tr>
<td>Other</td>
<td>0.00%</td>
<td>0.00%</td>
<td>8.74%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

Table 8: District-wise response to personal message received from strangers

We shall now understand the experiences of cyber fraud and bullying faced by participants. While we are considering the analysis based on different types of cyber crimes, the questions were presented in the interview schedule in a manner that described the features of the crime/fraud, acknowledging the fact that participants may not be aware of the type of abuse they have been subjected to.

The participants were asked if they have ever received messages via any online medium asking them to click on the link provided in order to win a prize, watch a video, update KYC details etc. The intent was to analyse how common the phenomenon of phishing is. A teacher from Raisen shared that she once received a message that said that she is eligible to win Rs 25 lakh for which she needs to click on a certain link and pay Rs 25,000 first, which
would, supposedly, go to the manager at SBI. In another example of phishing, a teacher shared that her brother once received a call from someone claiming to represent a prominent mobile network service provider who said that his land had been chosen by the service provider to set up a cell tower and that towards this he needs to submit his KYC and bank account details. On suspecting something fishy, he decided to probe and asked for their office location. The caller shared that it was in Delhi. He then told the caller that he would visit the office personally for further details. The caller immediately turned down the idea saying he was out of station and that he would be travelling out of the country over the next few days. On further probing, he simply disconnected the call. Other prominent examples of phishing involve sending links asking for donations for social causes and towards treatment of patients requiring immediate treatment. Some teachers seem to have even fallen for these scams and they shared that post making donations they found out that these were bogus cases.

About 73% shared that they have received such links, and among them, 22.96% responded to the message by clicking on the link provided. Among those who responded, the following were the most common consequences: their social media account got hacked (12.60%), they lost money from their bank account (7.63%), they were redirected to a page and asked to make a payment (11.83%), the link to a video kept popping on their screen (6.87%) and their personal information got leaked (3.05%). Among those who suffered any of these mentioned losses though, only 12.61% filed a complaint at a police station and 30.63% changed all their passwords to avoid further issue. About 51.80% shared that they did not do anything as they were unsure of what to do in such a circumstance. Let us take a look at the district-wise analysis of the same.

<table>
<thead>
<tr>
<th>Response if they suffered a loss post phishing</th>
<th>Jalpaiguri</th>
<th>S 24 Parganas</th>
<th>Khunti</th>
<th>Udaipur</th>
<th>Jaipur</th>
<th>Deoghar</th>
<th>Bhopal</th>
<th>Raisen</th>
</tr>
</thead>
<tbody>
<tr>
<td>I filed a complaint at the police station</td>
<td>0.00%</td>
<td>26.09%</td>
<td>2.27%</td>
<td>4.00%</td>
<td>0.00%</td>
<td>7.14%</td>
<td>38.71%</td>
<td>35.29%</td>
</tr>
<tr>
<td>I changed all my passwords to avoid further issues</td>
<td>69.23%</td>
<td>56.52%</td>
<td>20.45%</td>
<td>12.0%</td>
<td>9.76%</td>
<td>32.14%</td>
<td>41.94%</td>
<td>47.06%</td>
</tr>
</tbody>
</table>
I did not do anything as I was unsure of what to do

<table>
<thead>
<tr>
<th></th>
<th>30.77%</th>
<th>17.39%</th>
<th>77.27%</th>
<th>84.0%</th>
<th>90.24%</th>
<th>60.71%</th>
<th>19.35%</th>
<th>17.65%</th>
</tr>
</thead>
</table>

Table 9: District-wise response to a loss as a result of phishing

The participants were asked if they have ever felt uncomfortable during any online interaction they had. This could relate to a communication exchange they had with someone online, any insecurity or fear they felt at any point, or unpleasant content they came across inadvertently or was sent to them on purpose.

The reason this question is significant in this context is that it provides perspective on people’s online experiences in general. Internet users are often unaware of the risks and dangers in cyberspace and may also be ignorant of types of abuse. Given the lack of conversations on the topic in general, people often do not know whom to approach in case of any unpleasant online experience and additionally, they are unable to call out the form of abuse they have experienced. We thus take the stance that if an internet user has ever felt uncomfortable during their time spent online, they have in fact faced some form of abuse, irrespective of whether they realised it or were aware of the type of abuse they were subjected to. As a matter of fact, 57.14% responded affirmatively to this question and the following graph depicts the district-wise response.

Graph 1: Feeling of discomfort during an online interaction, district-wise
It is seen that except in the cases of Jaipur and Udaipur, a larger number of participants in all other districts have faced discomfort or experienced something unpleasant at some point during their online interactions. It is unclear as to why the participants from Jaipur and Udaipur responded to the question in this manner as in subsequent sections of this chapter, we get to see that study participants from the two districts have faced abuse and fraud. As was mentioned in the first section of this report, these are limitations that exist when supervision of the organisation on data collection teams is not possible during field study. The following table depicts the nature of interaction that made study participants uncomfortable, district-wise.

<table>
<thead>
<tr>
<th>Nature of the uncomfortable online interaction</th>
<th>Jalpajurgi</th>
<th>S 24 Parganas</th>
<th>Khunti</th>
<th>Udaipur</th>
<th>Jaipur</th>
<th>Deoghar</th>
<th>Bhopal</th>
<th>Raisen</th>
</tr>
</thead>
<tbody>
<tr>
<td>I was contacted relentlessly</td>
<td>73.68%</td>
<td>86.49%</td>
<td>41.43%</td>
<td>56.0%</td>
<td>53.66%</td>
<td>80.00%</td>
<td>44.44%</td>
<td>33.33%</td>
</tr>
<tr>
<td>Personal comments were made about me on my social media profile</td>
<td>55.79%</td>
<td>8.11%</td>
<td>10.00%</td>
<td>36.0%</td>
<td>51.22%</td>
<td>37.14%</td>
<td>25.93%</td>
<td>0.00%</td>
</tr>
<tr>
<td>I was asked to share my pictures with sender</td>
<td>7.37%</td>
<td>18.92%</td>
<td>28.57%</td>
<td>28.0%</td>
<td>34.15%</td>
<td>20.00%</td>
<td>11.11%</td>
<td>16.67%</td>
</tr>
<tr>
<td>I was asked to meet sender in private</td>
<td>28.42%</td>
<td>25.68%</td>
<td>42.86%</td>
<td>16.00%</td>
<td>36.59%</td>
<td>22.86%</td>
<td>11.11%</td>
<td>0.00%</td>
</tr>
<tr>
<td>Someone shared sexually explicit content with me</td>
<td>14.74%</td>
<td>8.11%</td>
<td>54.29%</td>
<td>20.00%</td>
<td>43.9%</td>
<td>25.71%</td>
<td>3.70%</td>
<td>16.67%</td>
</tr>
<tr>
<td>Someone shared hateful/abusive content targeting me</td>
<td>17.20%</td>
<td>1.35%</td>
<td>1.43%</td>
<td>16.00%</td>
<td>26.83%</td>
<td>7.14%</td>
<td>7.41%</td>
<td>33.33%</td>
</tr>
<tr>
<td>Other</td>
<td>0.00%</td>
<td>0.00%</td>
<td>7.14%</td>
<td>0.00%</td>
<td>4.88%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

Table 10: Nature of uncomfortable online interaction district-wise
What was the response of the participants to these interactions? About 53% responded by blocking the sender, 31% told the sender that they were uncomfortable and asked them not to contact them again, about 25% ignored the message/sender, about 21% deleted the posts about them, 15.72% deleted their social media accounts and about 8% relented to the request of the sender after repeatedly saying, “No” to them. The following graph depicts district-wise response of the participants.

![Response graph](image)

**Graph 2: Response of participants to uncomfortable online interaction, district-wise**

It is unfortunate to see that while some participants responded to the uncomfortable interaction by deleting their social media account, some even relented to the request of the sender as they got tired of communicating their lack of interest. Of those who went through such an experience, 85.52% informed someone about it while 14.48% never spoke about it to anyone. Again, when asked who they had informed about the incident/s to (for those who did), only 11.89% informed the police or cyber police. Among those who did report a cyber crime though, we do not have much understanding on the status of their case or what happened as a response to reporting. Among the others, a majority (67.84%) confided in their friends about the incident/s while 29.73% informed their spouse or parent and 12.16% informed their teacher or a trusted adult.
The study set out to learn about any incidences of cyber bullying faced by the participants. They were asked if they had ever been made fun of by their friends or acquaintances or if anyone had ever shared their personal details online with an intention to embarrass, hurt or malign their reputation. 33.48% answered in the affirmative to this question.

The table given below portrays the experience of participants with cyber bullying in an age and district-wise fashion. We see that participants in all age groups (except for Jaipur) are susceptible to cyber bullying and that participants from all districts have experienced the same, although the degrees differ. Raisen and Bhopal seem to be exceptions but the data here reflects the lower sample size and the fact that only children were interviewed in these two districts. Thus, the numbers for age categories above 18 years in the two districts do not point to an absence of cyberbullying in these areas. In fact, five of the eight teachers interviewed in Bhopal shared that they had experienced cyber bullying. This points to the need for more large-scale studies on various cyber crimes and responses to understand the issue in-depth.

<table>
<thead>
<tr>
<th>Age group and district-wise experience with cyber bullying</th>
<th>Jalpaiguri</th>
<th>S 24 Parganas</th>
<th>Khunti</th>
<th>Udaipur</th>
<th>Jaipur</th>
<th>Deoghar</th>
<th>Bhopal</th>
<th>Raisen</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-18</td>
<td>33.87%</td>
<td>41.86%</td>
<td>33.33%</td>
<td>42.86%</td>
<td>28.57%</td>
<td>22.22%</td>
<td>96.55%</td>
<td>100.00%</td>
</tr>
<tr>
<td>19-25</td>
<td>33.87%</td>
<td>32.56%</td>
<td>40.00%</td>
<td>14.29%</td>
<td>0.00%</td>
<td>51.85%</td>
<td>3.45%</td>
<td>0.00%</td>
</tr>
<tr>
<td>26-35</td>
<td>32.26%</td>
<td>25.58%</td>
<td>26.67%</td>
<td>42.86%</td>
<td>71.43%</td>
<td>25.93%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

Table 11: Experience of participants with cyber bullying, district and age-group wise

The following table depicts their response to online bullying.
Table 12: Response to cyberbullying incident

<table>
<thead>
<tr>
<th>Response to incident of cyberbullying</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>I ignored the message/s</td>
<td>23.58%</td>
</tr>
<tr>
<td>I told them that I was uncomfortable and asked them to take down the message</td>
<td>24.02%</td>
</tr>
<tr>
<td>I deleted the post</td>
<td>12.23%</td>
</tr>
<tr>
<td>I deleted my social media account</td>
<td>10.48%</td>
</tr>
<tr>
<td>I blocked the person</td>
<td>27.51%</td>
</tr>
<tr>
<td>Other</td>
<td>2.18%</td>
</tr>
</tbody>
</table>

In terms of one's response to an incident of cyber bullying, we see that the responses were personal to each individual (as we shall see is the case with other cyber crimes as well) and that essentially there are no standard responses although these are crimes. The response to such an incident seems to depend on instinct rather than the ideal case scenario of a standardised response— that of reporting on the basis of legal provisions. This is due to mainly because of the lack of awareness of cyber crimes and reporting and redressal and serves as a call for action on the part of all stakeholders.

Of the five teachers from Bhopal who had experienced cyber bullying, one said that they ignored the message, while the remaining four deleted their social media accounts. It is unfortunate that some participants end up quitting social media in response to cyber bullying incidents while some manage to confront the bully and ask them to delete the content. While victims may resort to responses like deleting the posts, ignoring it, or blocking the sender, the damage is often already done and the victimisation and mental health repercussions for victims could continue for a long time. When people are forced to quit a part of their online activity altogether due to bullying, fear, insecurity etc., their freedom is essentially taken away and is a cause of great concern. This points to the need for education and awareness among internet users on digital etiquette and acceptable behaviours. Reporting and redressal are also important in this context in order to ensure that people who default are reprimanded, leading to deterrence in the long run.
Of all the participants, 28.30% said that someone has, at some point, pretended to be them online by creating a fake account in their name. Among those who have faced identity theft and impersonation, the following table shows the district-wise and age-wise data of victims.

<table>
<thead>
<tr>
<th>Age group (in years)</th>
<th>Jalpaiguri</th>
<th>S 24 Parganas</th>
<th>Khunti</th>
<th>Udaipur</th>
<th>Jaipur</th>
<th>Deoghar</th>
<th>Bhopal</th>
<th>Raisen</th>
</tr>
</thead>
<tbody>
<tr>
<td>13-18</td>
<td>34.48%</td>
<td>48.39%</td>
<td>53.33%</td>
<td>38.46%</td>
<td>16.67%</td>
<td>25.93%</td>
<td>96.77%</td>
<td>100.0%</td>
</tr>
<tr>
<td>19-25</td>
<td>31.03%</td>
<td>32.26%</td>
<td>13.33%</td>
<td>23.08%</td>
<td>16.67%</td>
<td>44.44%</td>
<td>3.23%</td>
<td>0.00%</td>
</tr>
<tr>
<td>26-35</td>
<td>34.48%</td>
<td>19.35%</td>
<td>33.33%</td>
<td>38.46%</td>
<td>66.67%</td>
<td>29.63%</td>
<td>0.00%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

Table 13: Percentage of those who experienced identity theft age-wise and district-wise

We see that women and children in all age groups under study are vulnerable to finding fake profiles of theirs online. The percentage of those from Bhopal and Raisen who have faced identity theft is extremely high in the 13-18 years age group. Again, the reason for the percentages for other age groups in these two districts being close to nil or absent is due to the fact that only children were interviewed during the data collection exercise there. Those whose identity had been stolen had found out about it mainly through friends. Since it is not always easy to find out if someone is impersonating one’s profile, it is important that people inform their friends if they see suspicious or duplicate profiles online. Among the study participants who found fake profiles online, 71.90% came to know about it when a friend or acquaintance pointed it out to them, 13.33% found out when they received a friend request from the fake profile and 10.95% found the fake profile while browsing the internet themselves. Of the teachers from Bhopal, six of the eight shared that they had experienced identity theft at some point. In four of these cases, they came across the fake profile while browsing social media. In response, they reported those accounts on the concerned social media site.
The following table represents what the affected individuals did in response to finding out about the fake profile.

<table>
<thead>
<tr>
<th>Response to seeing fake profile online</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>I reported the matter on the social media site and got the profile taken down</td>
<td>19.21%</td>
</tr>
<tr>
<td>I didn’t do anything as I was not aware of my options</td>
<td>33.00%</td>
</tr>
<tr>
<td>I deleted my social media account</td>
<td>12.81%</td>
</tr>
<tr>
<td>I made an official complaint with the police/cyber police</td>
<td>5.42%</td>
</tr>
<tr>
<td>I asked my friends to not respond to any requests from that account</td>
<td>27.59%</td>
</tr>
<tr>
<td>Other</td>
<td>1.97%</td>
</tr>
</tbody>
</table>

**Table 14: Response to seeing fake profile online**

Here too, we see that only a minuscule percentage (5.42%) of the victims chose to file official complaints regarding impersonation and identity theft. This often points to ignorance regarding the dangers of having one’s identity stolen, in addition to the lack of awareness on how to respond to it. Those who indulge in such unlawful activity do so in order to commit fraud or to abuse/take advantage of someone online. Victims of identity theft often do not realise its repercussions unless they get into trouble as a result of someone impersonating them to take advantage of a third person. They then bear the additional burden of having to prove their innocence and get into long-drawn investigations leading to much stress and trauma.

**Exposure to inappropriate content**

The participants were asked if anyone had ever shared content (video/audio clips, messages, images etc.) with them online which made them uncomfortable. 47.93%
participants shared that they had, in fact, received some objectionable material at some point of time.

The following graph depicts the study participants’ exposure to inappropriate content. While participants from Jalpaiguri, Khunti, Bhopal and South 24 Parganas districts have faced this form of online abuse, in that more participants have faced the abuse when compared to those that haven’t, this is not the case with those from Deoghar, Jaipur, Raisen and Udaipur districts. With the latter districts we see that the number of those who have not seen inappropriate content online exceeds those who have.

![Graph 3: Participants’ experience of exposure to inappropriate content, district-wise](image)

What was the response of the victims to such content? Only 6.65% of the victims filed an official police complaint while 8.96% reported the content on the platform or site. About 40% ignored the post and 29.19% confronted the sender and asked them to take down the post. Almost 19% warned their friends about the sender, 8.38% deleted their social media accounts and finally, 13.01% did not do anything as they were unsure of what to do.

What was the nature of the inappropriate content shared with the victims? The following table depicts this. The data from the study shows that the inappropriate content was
predominantly abusive or with strong language and content that was sexual in nature and that portrayed women in a disrespectful manner. Again, one may notice that the percentage points don't add up to 100% as participants were allowed to choose multiple options. This is meant to acknowledge the fact that some content may be objectionable for different reasons and also that participants may have been exposed to multiple such content.

<table>
<thead>
<tr>
<th>Nature of objectionable material</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abusive/strong language</td>
<td>56.61%</td>
</tr>
<tr>
<td>The content degraded and was disrespectful of women</td>
<td>30.75%</td>
</tr>
<tr>
<td>The content was sexual in nature</td>
<td>39.94%</td>
</tr>
<tr>
<td>The content was violent in nature</td>
<td>13.51%</td>
</tr>
<tr>
<td>The content had hateful information directed at a community</td>
<td>8.62%</td>
</tr>
<tr>
<td>Other</td>
<td>0.29%</td>
</tr>
</tbody>
</table>

Table 15: Nature of inappropriate material

44.59% of the study participants shared that they had been, at some point, stalked by a friend, acquaintance or stranger online. This entailed someone known or unknown constantly 'liking' one’s posts even if it had no bearing on them, posting on the victim's wall/timeline or messaging one often in an unwelcome manner making them feel scared, embarrassed or uncomfortable. Of the eight districts under study, four of them have more participants who have not faced cyber stalking namely, Udaipur, Jaipur, Deoghar and Raisen.

During the focus group discussion with the teachers of Raisen district, a perplexing example came up that involves multiple forms of abuse including cyber stalking, online grooming and bullying. A teacher shared that her house help's grandson who is around 15-16 years of age
once got friendly with a much older woman from Himachal Pradesh on social media. They eventually became very close and the woman said that she wanted to marry the boy. The boy was so smitten by the woman that he stole money from his parents and attempted to elope multiple times but somehow never managed to get past Bhopal. Later, this woman reached his house claiming that they were in love and that she would stay at his home as his wife. The boy’s family tried to reason with her for three days but she would not leave. Finally, on the suggestion of the teacher, the boy’s family told her that this matter would be decided by the Sarpanch and the police. Three days after the conversation, the woman left stating that there was some emergency that she needed to attend to post which she has not returned or contacted the boy.

The district-wise data on incidence of cyber stalking is represented in the graph below.

![Graph 4: District and age-wise participants' experience with being stalked online](image)

Again, the study findings point to the lack of retaliation by victims to their experience of cyber stalking. Only 12.08% of the victims placed an official complaint with the police and 16.31% reported the perpetrator on the social networking site. The others responded by blocking the person on the platform (39.58%), confronting the stalker and asking them to stop stalking as it made the victims uncomfortable (23.56%), avoided taking any action
hoping the stalker would eventually stop pursuing them (45.32%) or avoided retaliation due to fear that the stalker would harm them or their loved ones (21.75%).

As we will see in other parts of this report, it is interesting to note that reporting of abuse/fraud depends on the circumstance. People in general seem more willing to report a cyber crime when there is a loss of money or in other words, in cases of financial fraud. Reporting also depends on the type and degree of abuse. Unless the abuse is extreme in nature, victims often end up suffering in silence and succumbing to the advances or actions of the perpetrator.

Knowledge, Perception and Practices: Participants in Cyberspace

Who would a study participant confide in if they were to go through an uncomfortable experience online? The answer to this is telling of who one trusts to not judge them, be able to respond appropriately and provide them the right advice on next steps to be taken, should they wish to do so. 52.47% of the study participants shared that at some point they have confided in someone about an uncomfortable experience they had online. Who, though, did they choose to turn to? The following table presents the results.

<table>
<thead>
<tr>
<th>Person victim confided in when faced with an uncomfortable situation online</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A close/trusted friend</td>
<td>64.52%</td>
</tr>
<tr>
<td>Spouse</td>
<td>12.08%</td>
</tr>
<tr>
<td>Parent/guardian</td>
<td>10.03%</td>
</tr>
<tr>
<td>A trusted adult or relative (other than parents)</td>
<td>4.63%</td>
</tr>
<tr>
<td>Teacher/mentor</td>
<td>0.00%</td>
</tr>
<tr>
<td>Sibling/cousin</td>
<td>8.74%</td>
</tr>
</tbody>
</table>

Table 16: Person participants confided in regarding uncomfortable online interaction
Let us take a slight detour before discussing the results presented above. It is important for children to have a wider social network, along with their immediate family members, as a support group. It is good for families to discuss and agree on who the children could or should turn to, apart from immediate family, in case they are in need of support. This ensures that children have trusted adults they could turn to for specific advice or support, as and when required, in case their immediate family is not at hand. At the same time though, it is important that parents are in a position to extend support to their children, hear them out, and help them overcome hurdles. The findings above show that children and women prefer turning to friends when they face an uncomfortable situation. While this is not undesirable in itself, what could be prompting them to do so?

We see that an overwhelming majority of the participants who did confide in someone about an uncomfortable online interaction chose to inform a close or trusted friend (64.52%). Only 22.11% confided in their spouse or parents and sadly, no one informed their teacher about the abuse they faced. Given that parents, teachers and spouses are the primary stakeholders in the lives of women and children, it is quite telling of our participants’ (and possibly that of our society at large) levels of trust and comfort. Why is this the case and how can this be overcome?

We also asked the participants how their parents or spouse would respond if they were to know of some abuse or fraud faced by them. The following table represents their responses. Although 54.91% shared that their spouse/parents would be supportive and would help them, almost 45% shared that they would either respond negatively or in a neutral manner. One can safely assume that participants chose to provide the answer that seemed socially acceptable, since it is not consistent with their actions. We see that in a majority of cases, participants chose to not inform their closest family members when they actually faced trouble online.

<table>
<thead>
<tr>
<th>Participants’ perception of response of parents/spouse to an issue they may face online</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>They would be supportive and do whatever it takes to protect or help me (including filing an official complaint)</td>
<td>54.91%</td>
</tr>
<tr>
<td>They would ignore the issue as they wouldn’t feel it is very harmful, serious or risky</td>
<td>9.64%</td>
</tr>
</tbody>
</table>
They would feel helpless as they won’t know ‘how to help or what to do 8.73%
They would get angry with me and blame me for what happened 18.18%
They would take away my device 6.91%
Other 1.64%

Table 17: Participants’ perception of response of parents/spouse to any online abuse/fraud they may face

The observation shared above that participants often share acceptable or desirable answers to questions regarding hypothetical issues is consistent with their responses to another question. In another part of the interview schedule, they were asked about who they would turn to if they were to face cyber abuse or online fraud. 50.53% shared that they would file a complaint with the police or cyber police, 43.92% shared that they would inform a parent/trusted adult/teacher/mentor or spouse, 30.20% said they would turn to a tech-savvy friend or acquaintance who would be able to help them, 26.71% would confide in a close friend and finally, 15.93% shared that they would inform a sibling.

There are two plausible explanations for this form of response which is inconsistent with their actual action in the past. One, as observed above, is that the participants felt compelled to give socially acceptable answers to the interviewers, and secondly, it could point to a positive development that has occurred in the course of the interview, i.e. that the questions have prompted them to give thought to the issue, resulting in increased motivation and confidence to follow formal procedures for redressal in the future. Although one cannot authoritatively conclude the latter, we will see later in the report that many study participants not only appreciated the topic of study and the questions, they also expressed interest in learning more and educating those around them about cyber abuse.

Together with the findings above, it is pertinent that almost 70% of the participants (69.83%) shared that their parents or spouse have expressed disapproval to their usage of the internet or electronic devices. The reasons are varied and are represented below.

<table>
<thead>
<tr>
<th>Reasons for disapproval to internet/device usage</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>They think it is a waste of time/ they say I spend too much time online</td>
<td>65.64%</td>
</tr>
</tbody>
</table>
They feel time spent online is never productive or beneficial in any way 38.80%
They simply don’t understand why I use the internet or what I do online 31.27%
They feel it disrupts other productive activities or my health 45.37%
They feel/say that it is unsafe and needs to be used minimally/sparingly 56.56%
Other 3.28%

Table 18: Reason/s for parental/spousal disapproval to internet/device usage by participants

The table shows that while many of the reasons parents or spouses disapprove of the usage of the internet or electronic devices by their wives or children are valid and relevant, there may be a gap in their understanding of the need for it in today’s world. While as a parent, one needs to ensure that children and especially teenagers do not get addicted to the internet, it is equally important that all stakeholders are brought on the same page regarding both the advantages and disadvantages of the internet. While technology and the internet are great enablers, education and awareness are required among all stakeholders to ensure that the benefits are reaped while users stay away from harm and addiction online. In fact, 90.25% of the participants shared that they too feel that there are disadvantages to internet usage. It is heartening thus, to see that the participants are cognisant and aware of the ill-effects of the internet. The following graph depicts the disadvantages of the internet as shared by the study participants. The term ‘internet persona’ used in the graph refers to one’s internet or online identity. It is a social identity that an internet user establishes in online communities and websites. This may be a deliberately constructed identity which is different (widely or at a smaller degree) from their real personas. Note that participants could choose multiple perceived disadvantages and hence the percentages don't add up to 100%.
In order to understand the participants’ perception on women’s and children’s online vulnerability, they were asked if they felt that women and children are more prone to facing abuse or being taken advantage of online, in comparison to men. An overwhelming majority, i.e. 91.32%, shared that they do indeed feel women and children are more vulnerable to abuse online. The table given below shows the various reasons they chose for the same. Again, since participants were allowed to choose multiple options, the percentage points do not add up to 100%.

<table>
<thead>
<tr>
<th>Reasons for vulnerability of children and women</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Children and women are generally not tech savvy (they are not equipped to efficiently use the internet and can therefore make mistakes that land them in trouble)</td>
<td>76.28%</td>
</tr>
<tr>
<td>They trust people easily or are extremely gullible emotionally and hence can be duped without difficulty</td>
<td>77.49%</td>
</tr>
<tr>
<td>Cyber criminals are usually men and they therefore take advantage of women and young children online</td>
<td>62.39%</td>
</tr>
<tr>
<td>Other</td>
<td>3.93%</td>
</tr>
</tbody>
</table>
Table 19: Reasons for children and women being more vulnerable to online abuse as per participants’ perception

Knowledge of abuse among participants’ friends and acquaintances

The participants were additionally asked questions about their knowledge of cyber abuse experiences of their friends, relatives and acquaintances. 44.46% shared that someone known to them had faced cyber abuse in the past.

Graph 6: Participants’ knowledge of abuse/fraud experiences among acquaintances

What, according to the participants, did their acquaintances do as a response to the fraud or abuse they faced? The participants shared that in 50.63% cases their acquaintances responded by changing all account passwords, did a factory reset of their device, deleted their account or suspended the account temporarily. 28.93% filed a complaint with the police or cyber police, 22.64% blocked and reported the person/content on the platform and 14.47% confront the abuser. Finally, 11.64% informed their bank, indicating a financial fraud they had experienced. It is often seen that victims often resort to informing the bank or approaching the police and cyber police primarily in cases involving financial fraud and loss of money from one’s account.
The participants were also asked about their knowledge of trafficking and other heinous crimes that have happened in their locality following a friendship or relationship that began online. Significantly, 32.04% of study participants responded that they know someone who was contacted online by an unknown person and then forced into some form of exploitation. The following table represents the type of abuse victims of such interactions were forced into.

<table>
<thead>
<tr>
<th>Type of exploitation faced</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human-trafficking for sexual exploitation</td>
<td>27.08%</td>
</tr>
<tr>
<td>Trafficking for labour</td>
<td>26.25%</td>
</tr>
<tr>
<td>Bonded labour</td>
<td>2.50%</td>
</tr>
<tr>
<td>Child labour</td>
<td>11.25%</td>
</tr>
<tr>
<td>Other</td>
<td>0.42%</td>
</tr>
<tr>
<td>Unsure</td>
<td>32.50%</td>
</tr>
</tbody>
</table>

Table 20: Type of exploitation post online interactions

What happened to the victims of such abuse? This is depicted in the following graph.

Graph 7: Consequence of the incident/s of trafficking/exploitation
In the above-given graph, “Other” includes cases in which the participants were not sure of the consequences or chose not to answer. These constitute a majority of the case. In 11 cases though, the participants shared that though the victim was not rescued, they are in touch with their family. While there is no clarity on why they have not been rescued or how they have managed to stay connected with their families, one possibility is that of cases where the victim has been married to the abuser.

**General questions to participants on the topic**

Apart from the questions on participants' experiences and responses to online abuse and fraud, they were asked some general questions about their awareness and opinions on the topic. They were asked if they knew whether or not such crimes came under the ambit of existing laws. The intention was not to check their knowledge specifically on the legal provisions but to prod them to think about the magnitude of these crimes and how one could legally respond to them. To this question, a majority of participants, i.e. 76.44%, shared that they are aware that these abuses and crimes are punishable by law in India. Finally, on being asked if they felt education and awareness are crucial for stakeholders, an overwhelming majority (93.84%) shared that there is a need for people to be educated on safe internet usage.
Qualitative findings from the study

As with any study of this nature, often quantitative or multiple choice questions alone do not suffice in bringing out stories of exploitation and victimisation. Despite the topic being sensitive, the interview schedule included an open ended question at the end in order to capture any additional significant details the study participants would be open to share. The interviewer was also given an opportunity to record any pertinent observation they may have made in the course of a specific interview or that of their field exposure at a location as a whole. Though many participants chose not to share any additional details in this section, a few did, bringing to the fore much relevant information from the perspective of understanding the situation in the district or a specific location and also in making recommendations for intervention and action.

Firstly, the interview process itself turned out to be quite enlightening, as per the observations of both the participants and data collection team. Some members of the data collection team shared that having to conduct the field study, they ended up with a better understanding of cyber crimes and abuse. Some of them got back post their field experience to share that they had no idea of how grave the issue was, until they started interacting with people during field work and learning about their experiences. Similarly, many participants appreciated the initiative itself and spoke about the need for much training, education and
awareness building on usage of the internet for all users, especially women and children. Let us take a look at some of the experiences shared by participants at the end of their interview.

Many study participants shared the importance of knowledge on appropriate usage of the internet since it consists of both pros and cons. They shared that given the internet is an inseparable part of one’s life today, it is crucial that people are provided updated and regular information on how to use it. It is quite clear through multiple observations from participants that they had hitherto not given much thought about taking steps to keep oneself safe online but that the interview process itself enabled them to widen their perspective on the issue as a whole. A 17-year-old boy from Jaipur district who is a school student shared at the end of his interview that in order to protect people from cyber abuse, he will talk about the issue with his friends and neighbours. One of the study participants shared that they have realised, as a result of this study, the fact that both the government and civil society are taking steps towards addressing the issue. When a 23-year-old college student from Udaipur opined that one need to be alert while using the internet, she was essentially expressing her realisation that one must not take the process of internet surfing casually, even when online for entertainment purposes. Many others echoed her observation by sharing the need to be vigilant while using the internet and being watchful of children who use devices often. Quite a few shared about incidents of cyber fraud of which their relatives or friends had been victims, sometimes involving large sums of money. A 25-year-old working professional from Khunti district who uses the internet for over five hours a day confessed that she is, in fact, addicted to the internet and wanted to know how she could reduce her dependency on the same. The interviewer additionally said that her parents were extremely worried for her and unaware of how to go ahead with de-addiction. A school student from Khunti, 18, shared that she had once received a message stating that she had won a lottery and asked her to fill out some details to claim the same. She said that she was saved from getting duped as she happened to mention this to her parents who warned her against providing any details as the link could be associated with cyber fraud.

A 35-year-old woman from Khunti district who is a village head shared of many cases of trafficking for child labour, domestic work and bonded labour from their village. She said that traffickers often visit the village and manipulate parents into sending their children with them. She spoke of the need for awareness and shared that she did not know that traffickers also use online mediums for their operations. While it is known that women are often targeted online by people in order to shame or humiliate them, one female participant who
was a divorcee shared that her ex-husband resorted to defaming her on social media. An 18-year-old college student from Deoghar district shared that sexually explicit images have been shared with her many times. She also shared that a guy had a picture of hers that he used to blackmail her with. She said that she was so afraid of the threat that she refused to venture out alone anywhere for three months after which the guy stopped calling her. Pertinently, she shared that she was gripped with fear but did not tell her parents about it as they would’ve blamed her. Post the interview with said girl, the interviewer shared something striking. They said that girls in the age group of 13 to 18 years often suffer alone even after being victimised online due to lack of information while their male counterparts are carefree and without any fear. This points to the disproportionate and unfair degree of fear and trauma girls face in society, simply on account of their gender.

A college student from Deoghar district, 18, said that if she were to face any abuse online she would not inform anyone about it out of fear. She said that she uses a mobile phone without her parents’ knowledge as they have prohibited her from using one. The girl’s response to her parents’ restriction should not come as a surprise. Where unreasonable restrictions are placed, one often finds different ways to circumvent the same to either satiate their curiosity or simply to take risks with that which piques their interest. This is especially true of adolescents and teenagers as they are naturally wired to take risks and rebel. It is important that caregivers and children are able to agree with one another on what’s allowed and not when it comes to internet usage (as with other matters) as that keeps an open channel of communication and builds confidence and trust in the relationship. It also ensures that children feel free to approach their caregivers when in doubt or trouble. In order to foster healthy relationships between caregivers and children, the former will need to be involved in the lives of their children and students. In fact, a 15-year-old boy from South 24 Parganas
remarked to the interviewer after his interview, commenting that nobody had ever talked to him about these issues up until that point. This comment came from a boy who started using the internet around the beginning of the pandemic and spends about three to five hours daily on it. In fact, many participants shared similar thoughts when they said that the interview prompted them to give thought to these issues and enabled them to realise that they needed better awareness and sensitisation on the topic. Some others shared how the topic itself was novel and that people don’t talk about these issues. It is possible that people in these communities don’t realise how common cyber abuse is. Apart from having heard of a few instances here or there, the silence and even taboo around the issue probably keeps the topic under wraps.

In the process of the interviews, some participants expressed their hesitance to report cyber crimes due to the “hassle” involved in following-up with procedures, deeming it an almost pointless exercise. These comments pointed to the need for clear and prompt redressal processes so victims who come forward to file complaints are not left high and dry and end up lacking faith in the system altogether. A 17-year-old college student shared the example of his uncle who had been duped of money online, adding that he had not received redressal despite filing a police complaint. A 35-year-old homemaker from Deoghar district shared that in Madhupur town in the district, many people have fallen prey to financial fraud committed using the internet but that not all victims approach the cyber cell with a complaint as they perceive the redressal process to be a hassle.
There seems to be a certain level of tolerance to cybercrimes in general. One participant from Jalpaiguri shared that while it is disturbing for anyone to go through harassment on social media, if it goes too far the victim should lodge a complaint at the police station or take the help of someone who can support in reporting. Why would there be a certain level of tolerance to social media or internet harassment at all? Could it be that like others who have shared similar points of view, this participant too feels that it is better not to get into the hassle of official reporting? It is essential that awareness is additionally directed to socialise internet users to the idea that there should be zero tolerance to any form of abuse online.

Another factor is that women are often victimised on multiple levels. One of the participants from South 24 Parganas district is a survivor of trafficking. Apart from that she has been a victim of financial fraud as a result of which she lost all her savings when her bank account got hacked into. From her interview responses we also get to see that she has been a victim of other types of abuse online as well. It is possible that in certain cases, these are all interlinked. It is thus important to counter such violence and victimisation through education, awareness and opportunities for women to grow. Momentous efforts are required by all concerned stakeholders to ensure better safety and security of women in all spaces—online and offline.

As shared briefly in the study findings, teachers in general are not aware of or involved in any way with their students’ online activities. Some suggested that they do not share the dynamics with students where the latter would approach them in case they faced an issue online. They also feel they have no more agency than to give some broad advice in case a child approaches them with an issue. They feel that serious matters would not reach them anyway as parents and the appropriate authorities would deal with them. This points to the need for training and awareness sessions with teachers as a stakeholder group to enable them to understand the crucial role they play in the lives of their students as well as with respect to matters related to cyber crimes and their redressal.

As we have found through the quantitative and qualitative study findings, online victimisation of women and children from the rural areas under study is rampant. While we do not intend to ignore the fact that even men can and do face cyber fraud and abuse, women and children are often disproportionately victimised. Having received an understanding of how abuse affects the population under study, we shall now move on to the recommendations section.
Recommendations of the Study

As with any study of a similar nature, this project has thrown up significant findings that have value not only in that it increases the knowledge base on the topic at hand, but also in that it presents issues that call for a concerted effort from various stakeholders. The overarching responsibility that rests with those that design such a study is to examine the approach that needs to be taken to address the issue and implement solutions- in this case, to reduce prevalence of cyber crimes and enable increased reporting and efficient redressal and additionally to engage in advocacy and action towards ensuring that perpetrators are called to account, thus acting as a deterrent to others. Such a tall order surely calls for a collaboration between different stakeholders. Let us now consider some broad recommendations based on the study findings.

The need for awareness and capacity building on the topic for all stakeholders involved

One of the primary findings of the study is the need to provide education and awareness to all users of the internet- particularly women and children- given their higher vulnerability to abuse online. Internet users need to be empowered with knowledge on safety and security tools available on various platforms as also reporting mechanisms available to them. Online
etiquette and best practices need to also be shared with them so internet users can avoid inadvertently becoming perpetrators of abuse online (such as cyber bullying).

**Encourage, promote and normalise conversations and discussions on cyber abuse**

Conversations on safe internet usage, etiquette and good practices are paramount. Along with awareness sessions, institutions like schools and colleges should encourage conversations on the topic by providing safe spaces for children and students to discuss issues and experiences. This is crucial to normalise talking about abuse and to give victims the confidence to come forward to report and the courage to follow through on the redressal process. This also enables people to be more understanding and accepting of online issues, thus ensuring people know better than to shame or blame victims.
Peer-group trainings and support groups in institutions and community

As we've seen based on the study findings, people prefer to turn to friends and peers when faced with abuse or other issues online. It is important that this is capitalised on by institutions and community for its benefits by ensuring creation of and training sessions for peer-groups that act as support groups and self-remedial systems among peers. Through these groups, one can groom young champions of cyber safety who play a significant role in educating and supporting those around them. This will play a crucial role in addressing prevention and redressal of cyber crimes.

Ensure reporting of cyber crimes
While victims of cyber crimes and abuse hesitate to report the abuse due to fear, trauma, shock and other reasons, it is necessary to ensure that the abuse gets reported anyway. Friends, family members and caregivers have a crucial role to play in this context. Along with awareness about cyber crimes and reporting mechanisms, systems need to be in place to guide children, students and adults alike to get guidance on such issues and help with reporting through support groups in institutions and communities.

**Educating caregivers, parents/guardians and teachers**

It is extremely important that stakeholders such as parents and other caregivers are educated on the pros and cons of digital technologies and also on the role they can play to ensure their children or students are able to reap maximum benefits while staying away from trouble. The fact that caregivers often feel challenged when it comes to the use of modern technology could result in an approach that restricts their students'/childrens’ freedoms. This is a primary reason for children resorting to using devices or the internet without their parents’ knowledge. There is a need to bridge this knowledge gap so their children and students do not fall behind due to their ignorance or ill-informed opinions. At the same time, children and students in general should be encouraged to form a social circle consisting of trusted adults, teachers and others who they can turn to in case their primary caregivers are unavailable or unable to guide them.
Efficient and convenient reporting mechanisms

Not only should reporting mechanisms including those on online platforms, official portals, helplines and physical spaces such as cyber crime police stations be made well-known but the systems should be efficient, the process seamless while ensuring confidentiality of the victim. Additionally, there need to be committees in schools and colleges that are equipped to handle and direct such cases, by providing victims with all the information and support they need to place and follow-through on their complaints.

Transparent and quick redressal processes
Victims often hesitate to report abuse as it could result in them being forced to relive and recount the trauma multiple times. Efficient investigation and legal processes are required to ensure that redressal is always victim-centric and in their best interest. This also needs to be communicated effectively with all stakeholders, especially victims, so that victims and their support systems do not get disillusioned or worse, apathetic towards the redressal process. This includes the need for education, awareness and training of law enforcement officials.

The need for counselling services for victims of cyber abuse

Along with support with reporting and redressal, victims also require counselling in several cases. While the former can be provided by friends and family members, trauma-informed counselling needs to be provided to victims by certified mental health professionals. Just as in the case of victims of other forms of abuse, those who have undergone severe abuse online often continue to live in fear, guilt and shame which needs to be dealt with. Hence, this service is crucial and needs to be made available for victims of cyber abuse.
Collaboration of all stakeholders to address rising cyber crimes

The involvement of different stakeholders is absolutely crucial in addressing the prevention and redressal of cyber crimes. Apart from children, caregivers and teachers and institutions like schools, colleges and CCIs who need to take initiatives towards educating and creating support groups, other stakeholders like the government, industry and all players in the sector at large have responsibilities towards ensuring that online spaces are safe for children.

Rural-area specific prevention strategy to tackle abuse

All concerned stakeholders should draw out a strategy specific to the local circumstances towards tackling cybercrime. Cyber abuse and fraud needs strategic interventions specific to the experiences of women and children located there. It will need to be dealt with differently
from other crimes existing in the area. Cybercrime cannot be tackled with a one-size-fits-all approach. Preventive measures need to be implemented in order to contain abuse.

**Helplines numbers to be popularised**

It would be helpful to make helpline numbers such as the one of Childline- 1098, and cyber crime helpline number- 1930, well-known in rural areas. Helpline numbers could be the most accessible and immediate form of reporting for women and children when it comes to various crimes they face. It is not only quicker than placing online or offline written complaints, but is also more accessible, and less intimidating a medium for people who need immediate assistance or advice.
Conclusion

This study set out to explore the trends in online abuse and trafficking of women and children and their vulnerability to online abuse in rural and semi-urban communities. It did so through interviews with women and children in the age bracket of 13 to 35 years in rural and semi-urban districts of Jharkhand, Rajasthan, Madhya Pradesh and West Bengal. Despite the sensitivity of the topic itself, many participants came forward to share details of their online experiences with the interviewers. The study additionally threw up findings on how women and children respond to such abuse and how it impacts them.

At the outset, we would like to point out that while online abuse of women and children in rural areas of India is common, it has not yet gained the attention it deserves with all concerned stakeholders. We have seen through this study that a small sample has yielded such a high instance of exploitation and vulnerability, thus pointing to the need for outreach in these areas in the form of training and awareness sessions involving different stakeholders such as women, children, parents and caregivers, teachers etc.
Broadly, we have been able to establish that secondary literature on the topic aligns with the findings of the primary research this project undertook. Women and children are increasingly accessing the internet for various purposes and consequently, they are also falling prey to fraudsters and perpetrators of online abuse. The lack of education and awareness on the topic renders them highly gullible and vulnerable to various forms of abuse. A respondent put across this point quite eloquently in sharing that one enables cyber criminals through ignorance. Lack of information on reporting and redressal has ensured that the issues remain grossly underreported and that perpetrators continue their operations in almost complete abandon. The participants, especially those from West Bengal, shared that they are aware of instances where people in their locality were contacted online by strangers who then exploited or trafficked them.

The report also points to the emotional and mental effects of abuse on victims. Not only does it lead to fear, shame and guilt, but victims often refrain from informing their family members about the abuse, leaving them to suffer alone. The generation gap between parents and children was also seen by way of which there is a lack of understanding, agreement and conversations around the safe and effective usage of technology. This also forces some children to keep their online activities (and abuse) under wraps for fear that they will be blamed for the experience.

Based on the findings of the study, various pertinent recommendations have been made. No one is immune to cyber abuse but women and children are disproportionately affected, calling for much focus and attention by different stakeholders towards protecting them. Based on the findings of this study, it is clear that cyber abuse and online trafficking are topics that need to be addressed not just in Tier 1 and metropolitan cities and that consequently, children and women need to be provided awareness and equipped on how to keep themselves safe. This requires concerted effort on the part of primary stakeholders such as children, parents/caregivers, educators and school management as well as providers of online services for children, the government, civil society and tech companies.
References


   https://www.freepressjournal.in/bhopal/madhya-pradesh-to-have-first-cyber-sakhis-in-harda


22. Bhopal: 1,341 women were abducted for marriage in MP in 2021, says NCRB. (2022, August 30). *The Free Press Journal.*
23. Bulli Bai case: ‘Level of depravity is shocking’. (2022, Jan 05). The Hindu


26. Domestic violence against women: MP tops the chart. (2019, October 23). The Times of India


30. Govt defines child pornography brings digital or computer generated content under it WCD Ministry. (2020, April 4). *The Week*. 
https://www.theweek.in/content/archival/wire-updates/national/2019/07/11/des52-wcd-child%20pornography.html

31. India reported 11.8% rise in cyber crime in 2020; 578 incidents of ‘fake news on social media’: Data. (2021, Sept 15). *The Hindu*. 


https://www.counterview.net/2022/07/kailash-satyarthi-ngo-rescues-10-tribal.html


38. Rajasthan: Cases pile up in districts due to absence of experts. (2021, Apr 30). *The Times of India.*


41. This town in Jharkhand is the cybercrime capital of India. (2018, Jun 1). *Deccan Chronicle.*


43. 45% growth in active internet users in rural India since 2019: Study. (2022, May 5). *Business standard.*

44. 400% Increase in Cyber Crime Against Children in 2020 vs 2019, Most Cases of Sexual Abuse. (2021, Nov 14). *News18.*

45. 5,000 child pornography cases being probed by SOG in Rajasthan. (2021, Dec 15). *The Times of India.*
Changing Trends in Online Abuse and Trafficking of Women and Children

Appendix: Interview Schedule Employed for the Study

Survey on Online Abuse and Trafficking

Note for the participant (to be verbally shared by the data collector/interviewer): Hello! We are conducting a survey regarding internet usage and online abuse on behalf of two organisations namely, Space 2 Grow and CyberPeace Foundation. These organisations work in the areas of child protection, anti-human trafficking, promoting awareness on cybercrimes and protecting people from cyber threats and abuse. This survey will contribute to a study whose aim is to understand people's experiences online, especially with respect to online abuse. This interview will take about 20-30 minutes. You are free to not answer any question if it makes you uncomfortable but we would encourage you to answer as many as possible as this will help us understand current trends in your village/town/city so we can help your community better. Please be aware that your personal information will not be shared with any third party or published anywhere. These details are only taken to analyse the demographic for the purpose of the study. Do you have any questions at this point? Do you give your consent to being interviewed?

Note for the interviewer: Before beginning the interview, ask the participant (interviewee) about any experiences of abuse in general including physical abuse which may have been an extension of an online interaction. Feel free to add any relevant qualitative observations you have made and pertinent information shared by the participant. Where relevant, you can mark multiple answers for one question. Before starting the interview, explain the following concepts in brief so they are able to answer the questions appropriately. These definitions act as a guide for you to explain the concept to the participant. Please explain them in simple, conversational language for their benefit.

➔ **Cyber bullying**: Cyber bullying is bullying that happens online. It includes sending, posting, or sharing negative, harmful, false or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.
→ **Cyber stalking:** Cyber stalking refers to the use of the internet and other technologies to harass or stalk another person online and is an extension of cyberbullying and in-person stalking. Those who engage in cyber stalking use different tactics and techniques to harass, humiliate, intimidate and control their victims or targets.

→ **Child SExual Abuse Material (CSAM):** CSAM is any depiction of sexually explicit content involving a minor (a person under 18 years of age) and is a form of child sexual exploitation.

→ **Cyber grooming:** People who engage in CSAM often first ‘groom’ their victims or cultivate a relationship with a child and gradually sexualise the contact over time. Online ‘groomers’ are people who befriend children online to take advantage of them for sexual purposes. The grooming process fosters a false sense of trust and authority over a child in order to desensitise or break down a child’s resistance to sexual abuse.

→ **Impersonation and identity theft:** Impersonation and identity theft happens when someone steals your personal information and pretends to be you in order to commit fraud or gain other financial benefits.

→ **Phishing:** Phishing is a type of identity theft in which fraudulent emails or texts with links that look legitimate are sent to people. When someone clicks on such a link, it can steal your personal information. Examples of these include messages asking the user to click a link and enter personal information to apply for a job, win a cash prize, watch a video etc.
## Interview Schedule

<table>
<thead>
<tr>
<th>Name (optional):</th>
<th>Age:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sex: M / F / Other</th>
<th>Location:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Occupation:
- a. Homemaker
- b. School student
- c. College student
- d. Working professional
- e. Unemployed
- f. Other _____________

### Marital status:
- a. Single
- b. Married
- c. Separated/Divorced/Widow

### Educational qualification:
- a. Illiterate/Uneducated
- b. Primary (5th pass)
- c. Matriculate (10th pass)
- d. Senior secondary (12th pass)
- e. Student: ______
- f. Graduate
- f. Other: __________
1. Do you use the internet? Yes / No

2. If yes, how often do you use the internet?
   a. Daily
   b. 2-3 times/week
   c. 2-3 times/ month
   d. Once a month or less

3. On average, how many hours do you spend online every day (If participant answered option (a) above)?
   a. Less than 1 hour
   b. 1-2 hours
   c. 3-5 hours
   d. Over 5 hours

4. Since how many years have you been using the internet?
   a. 1-2 years
   b. 3-5 years
   c. 6-10 years
   d. Over 10 years

5. Which device do you use to surf the net?
   a. Mobile phone
   b. Laptop/PC
   c. Tablet
   d. Public computer (at a cybercafé)
   e. All of the above
6. Does the above-mentioned device/s belong to you? Yes/No

7. Where do you surf the net from?
   a. Home
   b. Public place
   c. School/College/Workplace
   d. All of the above
   e. Other ______________

8. For what purpose/s do you use the internet?
   a. For school/college work
   b. For professional work
   c. Social media
   d. Entertainment (Music and movies)
   e. Online gaming
   f. E-commerce (Shopping)
   g. For general information/news etc.
   h. All of the above
   i. Other ______________

9. Do you have a social media account? Yes / No

10. If yes, which one/s?
    a. Facebook       b. Instagram       c. Twitter       d. All of the above
    e. Other ______________
11. Have you ever received/do you receive friend requests from unknown people on any of these sites? Yes / No

12. If yes, how did/do you respond to them?

   a. I always accept those requests
   b. I always ignore/reject them
   c. I accept the request if I have common friends with the person
   d. I read the profile even if I don’t know the person and then accept if I feel like it
   e. Other: ______________________________________________________

13. Have you ever received personal messages from unknown people via SMS/Whatsapp/Messenger etc.? Yes / No

14. If yes, how did you respond?

   a. I read the message and responded appropriately.
   b. I read the message and ignored it/did not respond.
   c. I ignored the message/ did not read it
   d. I blocked the person
   e. Other: ______________________________________________________

15. Have you ever received messages via SMS/Whatsapp/Messenger etc. asking you to click on a certain link to receive a prize or to login to a social media account to watch a video or to give your personal information for banking purposes, to apply for a job etc.? Yes / No

16. If yes, how did you respond?

   a. I read the message and responded appropriately.
   b. I read the message and ignored it/did not respond.
   c. I ignored the message/ did not read it
   d. I blocked the person/number
17. If you did respond, what happened afterwards?
   a. My social media account got hacked
   b. I lost money from my bank account
   c. My personal information got leaked
   d. Nothing happened immediately
   e. I'm not sure
   f. The link was genuine and not a case of phishing
   g. Other ____________________________________________________

18. If you suffered a loss, what did you do?
   a. I filed a complaint at the police station
   b. I changed all my passwords to avoid further issues
   c. I did not do anything as I was unsure of what to do
   d. Other ____________________________________________________

19. Have you ever felt uncomfortable during any online interaction with a known or unknown person? Have you been harassed by someone online? Yes / No

20. If yes, what was the nature of the interaction?
   a. I was contacted relentlessly
   b. Personal comments were made about me on my social media profile
   c. I was asked to share my pictures with him/her online
   d. I was asked to meet him/her in private
   e. All of the above
   f. Other ____________________________________________________
21. If yes, what did you do?
   a. I ignored the message/s
   b. I told them that I was uncomfortable and asked them not to contact me
   c. I got tired of saying, "No" and finally relented to their request
   d. I deleted the posts about me
   e. I deleted my social media account
   f. I blocked the person
   g. Other ________________________________

22. Did you inform anyone about the incident/s?  Yes / No

23. If yes, who did you inform?
   a. I filed a complaint with the police/cyber police
   b. I told a friend about it
   c. I told my spouse/parents
   d. I told my teacher/a trusted adult
   e. Other ______________________________________________________

24. Have your friends/acquaintances made fun of you or shared personal details about you online with an intention to embarrass/hurt/malign you?  Yes / No

25. If yes, how did you respond?
   a. I ignored the message/s
   b. I told them that I was uncomfortable and asked them to take down the message
   c. I deleted the posts about me
   d. I deleted my social media account
   e. I blocked the person
26. Has anyone ever pretended to be you online by creating a fake account in your name?  
Yes / No

27. If yes, how did you find out about it? 
   a. A friend/acquaintance of mine told me about it  
   b. I saw the fake profile while browsing through my profile  
   c. I got a message/friend request from that account  
   d. Other: __________________________________________________

28. If yes, what did you do?  
   a. I reported the matter on the social media site and got the profile taken down  
   b. I didn’t do anything as I was not aware of my options  
   c. I deleted my social media account  
   d. I made an official complaint with the police/cyber police  
   e. I asked my friends to not respond to any requests from that account  
   f. Other ____________________________________________________

29. Has anyone ever shared content (pictures, videos etc.) with you online that made you uncomfortable?  Yes / No

30. If yes, what did you do about it?  
   a. I ignored the message/post  
   b. I told the sender that I was uncomfortable and asked them to take down the message/post  
   c. I reported the matter on the social media site and got the profile taken down  
   b. I didn’t do anything as I was not aware of my options  
   c. I deleted my social media account
d. I made an official complaint with the police/cyber police

e. I asked my friends to not respond to any requests from that account

f. Other ______________________________________________________

31. What was the nature of the content?

a. It used language that was abusive or strong language

b. The content degraded women and was extremely disrespectful of them

c. The content was sexual in nature

d. All of the above

e. Other: ______________________________________________________

32. Have you ever been stalked online by a friend/acquaintance/stranger (Did someone keep liking all your posts or keep posting on your timeline or keep message you in an unwelcome manner making you feel scared, embarrassed or uncomfortable?) Yes / No

33. If yes, what did you do about it?

a. I didn’t do anything as I was scared to retaliate (I felt I or my loved one/s could be harmed if I retaliated)

b. I didn’t do anything hoping the person would stop doing it eventually

c. I asked the person to stop doing it as it made me uncomfortable

d. I reported the person on the social networking site

e. I blocked the person on the social networking site

f. I made an official complaint with the police/cyber police

g. Other ______________________________________________________

34. Have you ever confided in someone about an uncomfortable interaction/experience you had online? Yes / No
35. If yes, who did you confide in?
   a. A close/trusted friend
   b. My spouse
   c. My parent/guardian
   d. A trusted adult or relative (other than parents)
   e. My teacher/mentor
   f. My sibling/cousin
   g. Other ___________________________________________________

36. How do you think your parents/spouse would respond if they came to know of some abuse/fraud you faced online?
   a. They would be supportive and do whatever it takes to protect or help me (including filing an official complaint)
   b. They would ignore the issue as they wouldn't feel it is very harmful, serious or risky
   c. They would feel helpless as they won't know how to help or what to do
   d. They would get angry with me and blame me for what happened
   e. They would take away my device
   f. Other ___________________________________________________

37. Have your parents/spouse ever expressed disapproval of your usage of the internet or your electronic devices?  Yes  /  No

38. If yes, what is the reason for their complaint/disapproval?
   a. They think it is a waste of time/ they say I spend too much time online
   b. They feel time spent online is never productive or beneficial in any way
   c. They simply don’t understand why I use it or what exactly I do online
d. They feel it disrupts other productive activities or my health (e.g., lack of sleep due to increased usage, it affects the eyes, it makes me behave differently etc.)

e. All of the above

f. Other ____________________________

39. Do you feel there are disadvantages to the use of the internet?  Yes / No

40. If yes, what would you say is the most pertinent disadvantage?

a. It can lead to addiction (you feel that you can’t go even one day without checking your social media account)

b. It makes you extremely dependent on it to get on with day-to-day activities

c. It makes people behave differently by trying to portray a different person to who they really are

d. It can be unsafe for children and women since they are especially vulnerable to being treated disrespectfully or being abused online

e. Too many people are using the internet to exploit/defraud/dupe other people and this is big threat to the users of the internet

f. All of the above

g. Other ______________________________________________________

41. Who would you turn to if you faced an online abuse (cyber bullying or stalking, impersonation and identity theft, CSAM, phishing etc.)?

a. I would file an official complaint with the police/cyber police

b. A parent/spouse/a trusted adult/teacher/mentor

c. A close friend

d. A sibling

e. A friend/adult/acquaintance who tech-savvy and would know how to help

f. Other ______________________________________________________
42. Do you feel women and children are more prone to facing abuse or being taken advantage of online?  Yes / No

43. If yes, what makes you feel they are more vulnerable?
   a. Children and women are generally not tech savvy (they are not equipped to efficiently use the internet and can make mistakes)
   b. They trust people easily or are extremely gullible emotionally and hence can be duped without difficulty
   c. Cyber criminals are usually men and they therefore take advantage of women and young children online
   d. All of the above
   e. Other ____________________________

44. Do you know anyone who has faced abuse or fraud online?  Yes / No

45. If yes, what was the type of abuse faced?
   a. Cyber bullying
   b. Cyber stalking
   c. Impersonation and identity theft
   d. CSAM
   e. Phishing
   f. Other ____________________________

46. If yes, what did they do in response?
   a. They changed all their passwords/did a factory reset of their device or deleted their account or suspended it temporarily
   b. They filed an official complaint with the police/cyber police
   c. They blocked the person/reported the person/post on the social networking site
   d. They directly told the perpetrator to stop the bullying/take down a post etc.
47. Do you know anyone who was contacted online by an unknown person and then lured into forced labour or other form of exploitation? Yes/No

48. If yes, what was the type of exploitation faced?
   a. Sex trafficking
   b. Trafficking for labour
   c. Bonded labour
   d. Child labour
   e. Other ______________________________________________________

49. If yes, what happened to the victim?
   a. The victim has been missing ever since
   b. The victim managed to contact a friend/family member and was rescued
   c. A complaint was placed in the police station and the police rescued the victim
   d. The victim was rescued by a social service organisation
   e. Other ______________________________________________________

50. Do you know that these offences are all punishable by law in India? Yes / No

51. Do you think it is important for people to be educated on how to use the internet safely? Yes / No

52. Would you like to share any experiences/thoughts on this topic with us?
    ____________________________________________________________
    ____________________________________________________________

53. Anecdotes/observations of the interviewer, if any.
    ____________________________________________________________