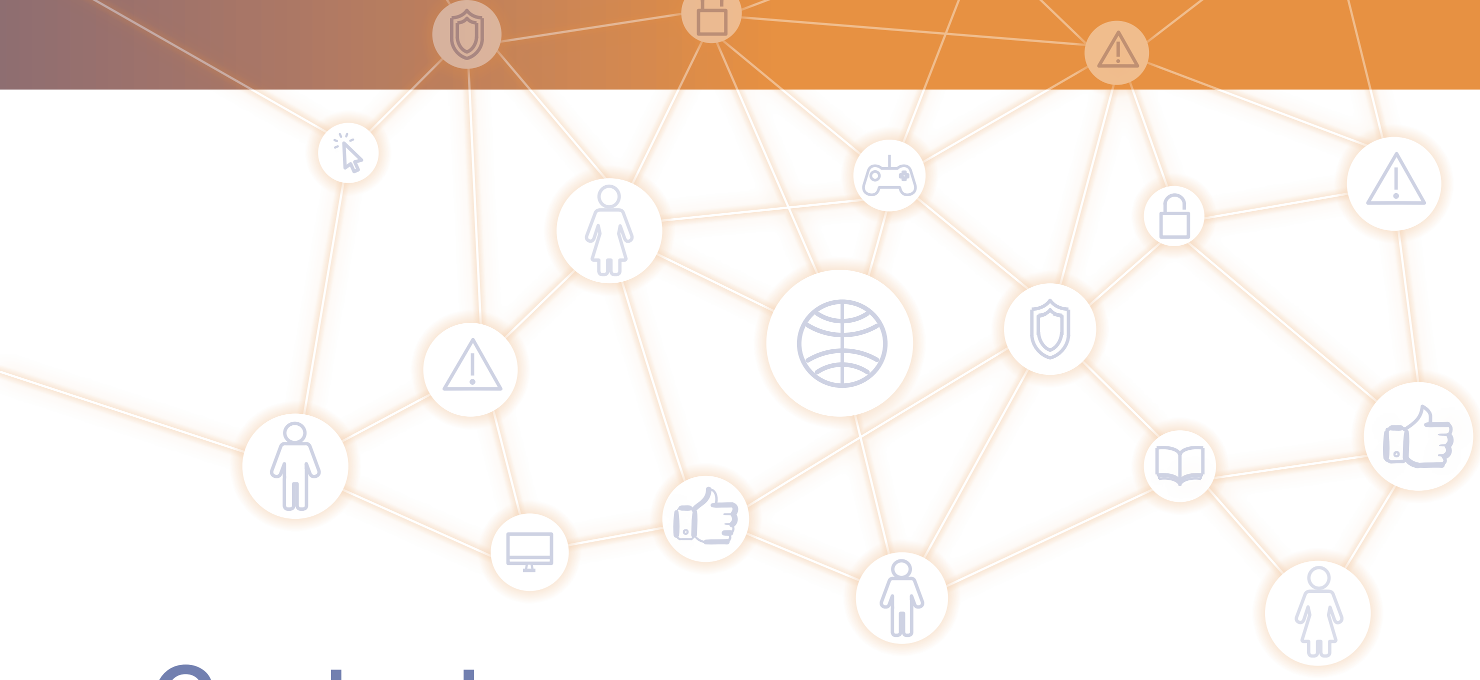
SPACE 2 GROW
IMPACT ACCELERATED

Supported by:

ON
OMIDYAR NETWORK INDIA

Digital Safety of Children:

Creating Safe Online Spaces



Contents

Acknowledgement

The authors are grateful to the following advisors for their guidance and input through discussions.

1. **Prof. Beulah Shekhar -** Chair Professor of Criminology at National Forensic Sciences University, Delhi.
2. **Dr. Eesha Sharma -** Assistant Professor in the Department of Child and Adolescent Psychiatry, NIMHANS.
3. **Ms. Linda Burch -** CEO, Alice Waters Institute (Ex Co-founder, Chief Strategy and Development Officer,Common Sense Media).
4. **Mr. Pulkit Jain -** Co-founder, Vedantu Innovations Pvt Ltd.
5. **Mr. Sameer Desai -** Video games industry specialist (Ex Country Head India, THQ Nordic).

The authors would also like to thank key teams for their valuable contributions to this report. They thank:

1. Omidyar Network India team
2. Space2Grow's Research and Analysis Team
3. How India Lives team
4. Kabuki Writers' Team

We also share our special thanks to the children, parents, educators, schools, law enforcement officers, media professionals, mental health professionals, academicians, industry representatives from gaming and edtech, representatives from regulatory bodies and policymakers, judges and lawyers who participated in our interviews and discussions for their valuable contributions towards the enrichment of the report.

We would also like to thank every single person within the ecosystem who is striving to empower tomorrow's digital citizens. One Safe Click At a Time!

If you would like to extend the conversation on digital safety and discuss this report, please contact the authors:

Chitra Iyer
Co-Founder and CEO, Space2Grow
Email - chitra@space2grow.in

Anuj Singhal
Co-Founder and Partner, Space2Grow
Email - anuj@space2grow.in

Before We Begin This Journey

"A friend of mine hatched up a friendship with a stranger on the internet. They would talk regularly. The person would express their desire to meet her very often. He was keen. A plan was almost made when she found out that the person had been lying about his identity. He, in fact, was a much older person. She blocked him immediately, but he stalked her by calling her on her mobile."

– 15 year old girl, Delhi

In embarking on this research endeavour, we ventured into the world of teens and preteens, seeking to understand their experiences in the digital realm. The narrative shared above is just one of the myriad of stories that unfolded during our interviews — a poignant reminder of the internet's dual nature. While on one hand, it represents joy and opportunity, on the other hand, it presents significant risks and harm.

Often, in the pursuit of rigorous analysis, researchers tend to rely on academic terminology such as 'sample size', 'target group', and 'case study'. While these terms serve a crucial purpose, they can inadvertently create a certain emotional detachment from the very subjects we seek to understand. In doing so, the starkness of statistics and data might overshadow the very real impact they hold for the lives of children.

It is imperative, therefore, to consistently remember that behind every statistic is a child. These numbers encapsulate the intricacies of their digital journeys, where risks encountered in the online spaces can profoundly shape their existence. As we dived into our findings, we made it our mission to maintain a grounded and compassionate approach to our research. We believe every child's experience is a narrative worth acknowledging, even if it amounts to a single data point. The suffering of one child is, and always will be, one too many.

Executive Summary

"Every child has the right to feel safe no matter where they are. We must not ignore the growing risks they face online: violence, bullying, harassment & exploitation."

-- **Antonio Guterres**, Secretary General, UN

In an era where the digital world seamlessly intertwines with the lives of 'Digital Natives' — children growing up in an era of ubiquitous internet usage — new opportunities as well as risks emerge. As online threats, including those of violence and exploitation loom, it becomes imperative to understand children's online experiences and navigate the evolving digital landscape they inhabit. This is the idea with which the research project 'Digital Safety of Children: Creating Safe Online Spaces' was initiated.

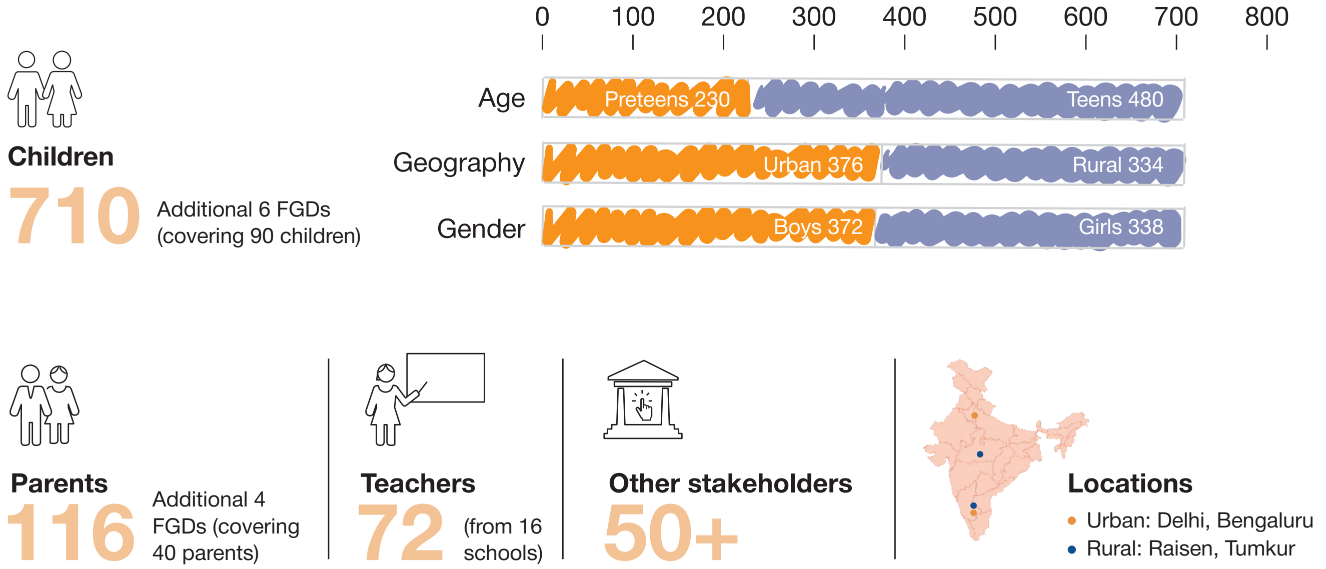
This study, by Space2Grow, supported by Omidyar Network India, aims to provide a holistic understanding of children's online behaviour patterns. It incorporates the perspectives of other key stakeholders (parents, teachers, law enforcement, technology companies, academicians, judiciary, lawyers, and government officials) who shape the digital safety ecosystem of children. It also provides insights on actions that can be taken to promote safer internet usage by children.

Research Methodology

The methodology was designed to encompass diverse perspectives and ensure an inclusive evaluation of the online safety landscape for children. It incorporated both qualitative and quantitative research methods, involving focus group discussions (FGDs), and in-depth interviews with over 700 children and over 100 parents, to gather valuable insights. This allowed for a deeper exploration of the experiences and viewpoints of the participants (Figure ES1).

Furthermore, in-depth interviews were conducted with other critical stakeholders, including teachers, law enforcement/government officials and judiciary, as well as industry experts, mental health professionals, academicians, and journalists. Additionally, existing knowledge and findings on the digital harms and safety of children at national and international levels were reviewed to complement the findings from the primary data.

Figure ES1: Research methodology



Source: Space2Grow research

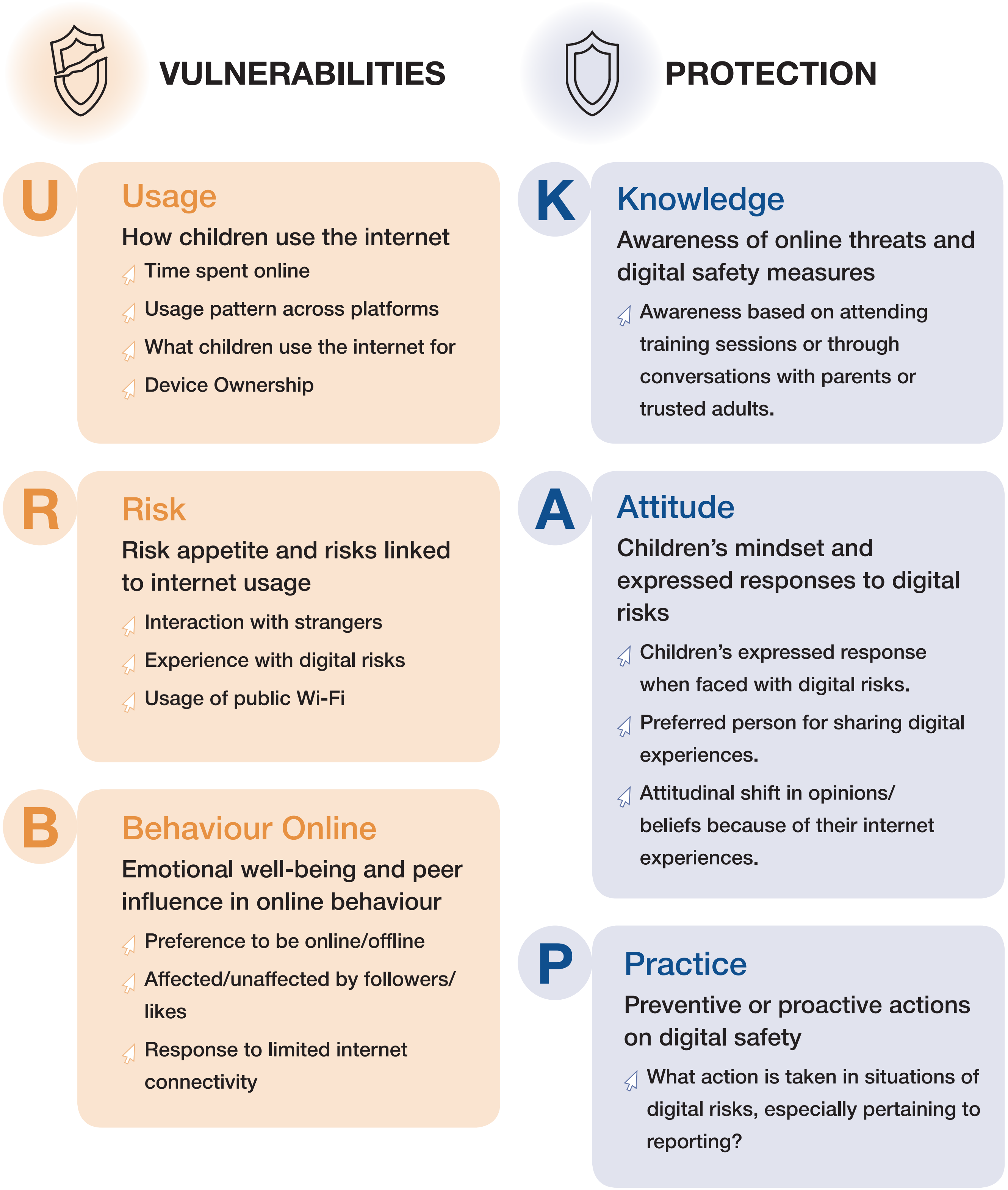
URBKAP Digital Safety Analysis Framework

As part of this study, Space2Grow has developed the 'URBKAP' framework. The framework offers a structured approach to assess the digital safety of children by employing a vulnerability versus protection matrix.

The vulnerability factors include children's internet usage, risks, and behaviour, whereas the protection factors include their preparedness and ability to address vulnerabilities in digital spaces, through knowledge, attitude, and practice. Additionally, it takes into account the response from parents and teachers as first responders and the perceptions of other key stakeholders — including the judiciary, police, lawyers, mental health professionals, non-profits, academia, media and government bodies.

The URBKAP Framework enables a holistic evaluation of the current state of child digital safety. It aims to empower policymakers and stakeholders to identify risks, address knowledge gaps, and make informed decisions regarding policies and interventions aimed at safeguarding children in the digital landscape (Figure ES2).

Figure ES2: URBKAP Framework



VULNERABILITIES

U **Usage**

How children use the internet

- Time spent online
- Usage pattern across platforms
- What children use the internet for
- Device Ownership

R **Risk**

Risk appetite and risks linked to internet usage

- Interaction with strangers
- Experience with digital risks
- Usage of public Wi-Fi

B **Behaviour Online**

Emotional well-being and peer influence in online behaviour

- Preference to be online/offline
- Affected/unaffected by followers/ likes
- Response to limited internet connectivity

PROTECTION

K **Knowledge**

Awareness of online threats and digital safety measures

- Awareness based on attending training sessions or through conversations with parents or trusted adults.

A **Attitude**

Children's mindset and expressed responses to digital risks

- Children's expressed response when faced with digital risks.
- Preferred person for sharing digital experiences.
- Attitudinal shift in opinions/ beliefs because of their internet experiences.

P **Practice**

Preventive or proactive actions on digital safety

- What action is taken in situations of digital risks, especially pertaining to reporting?

Key Findings

01 Usage

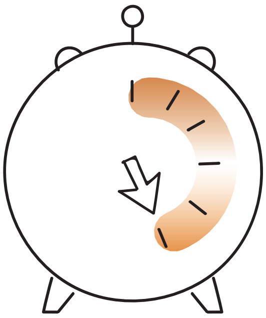
Striking similarities in internet usage by children and ineffective age-gating

The research findings on children's internet usage patterns reveal striking similarities among genders and across rural and urban environments. Despite concerted efforts within the industry, establishing effective age-gating measures is a persistent challenge.

Time on the Internet

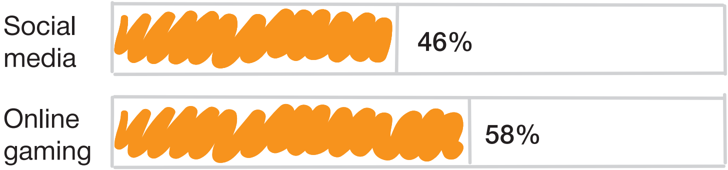
70%

1 to 5 hours daily



Source: Space2Grow research

Preteens accessing online platforms



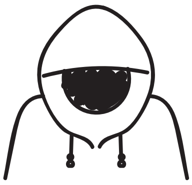
Notes/definitions:
1. As per the guidelines set by social media companies, the age to have an account is 13 years.
2. In accordance with the Indian legal frameworks Real Money Gaming requires the user to be 18 years and above.

02 Risk

Increasing online interactions with strangers coupled with a lack of safe spaces

Pre-teens and teens often interact with unfamiliar individuals on the internet. This exposes them to potential manipulation, harassment, abuse, deception, and even solicitation. Significant number of children have experienced a range of digital risks, whether while gaming, using social media, or engaging with educational technology platforms. Unfortunately, the absence of secure safe spaces hinders their capacity to effectively navigate and address these risks.

Interactions with Strangers



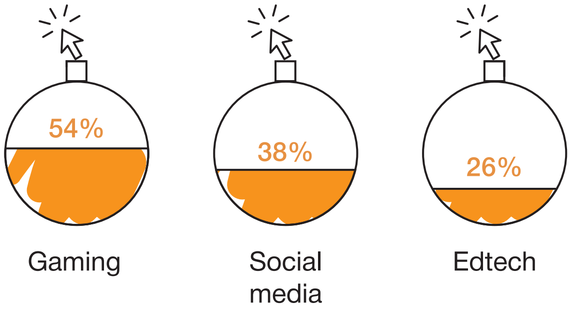
60%

of the teens who interacted with strangers online have later met them offline.

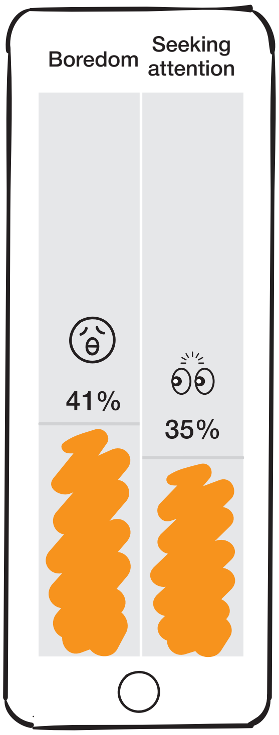
Notes/definitions:
3. Digital Risks: Any form of harm/risk/abuse faced by children on the internet (See Figure 1.5).

Source: Space2Grow research

Digital risk faced by children across platforms



Top motivators to be be online



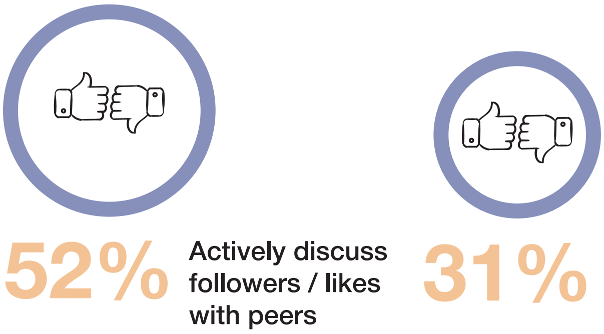
Source: Space2Grow research

03 Behaviour online

Curiosity and the need for social validation are key drivers for digital exploration

Children's online behaviour has seen a surge in digital exploration and risk-taking, driven by a combination of boredom and curiosity to venture into restricted content. The quest for validation in online spaces has resulted in children devoting a significant amount of time to internet activities. This trend has raised concerns among mental health professionals, who have observed an increasing impact on the mental well-being of children.

Social Validation

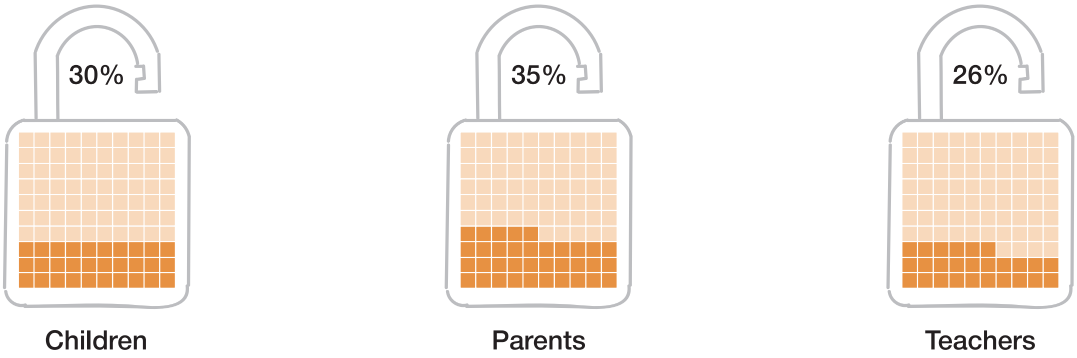


04 Knowledge

Limited knowledge and awareness regarding digital safety are causes for concern

There is a notable deficiency in children's understanding of how to safeguard themselves from digital risks, raising significant concerns. Parents and teachers also display limited awareness of digital safety, further compounding the issue.

Awareness of Digital Safety



Source: Space2Grow research

05 Attitude

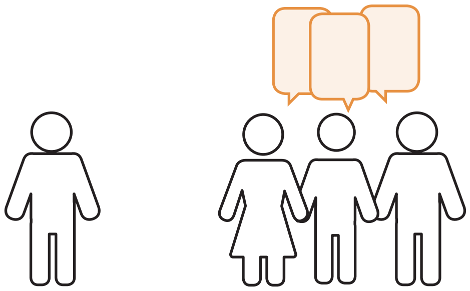
Reliance on peers and self-intervention to manage risks

Parents believe children would feel most comfortable discussing issues relating to digital harms with them or their guardians. However, when faced with risky situations in online spaces, children either seek assistance from their peers or address the situation on their own. This highlights a gap in the role of parents and teachers as the primary responders to digital risks faced by children.

Seeking Support

79%

of children prefer self-intervention or seek help from peers over involving caregivers or authorities



Source: Space2Grow research

06 Practice

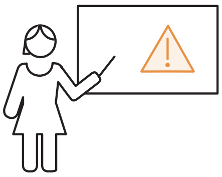
Lack of enabling strategies and limited recourse to law enforcement for redressal

Children tend not to make formal complaints or seek help from law enforcement and other official forums when faced with digital risks on account of low levels of knowledge on digital safety and fear of repercussions. Even when complaints are made, there is often a lack of coordinated response from stakeholders.

Complaints and Redressal

3%

Parents employ active techniques, like giving advice or diverting their child's attention to other activities, to manage their internet usage.



16%

Educators in school proactively reported digital risks faced by children to law enforcement

Notes/definitions:
Preventive Actions: Counselling, training and awareness sessions.
Proactive Actions: Reporting to law enforcement, reporting to platforms and taking action against perpetrators/accused.

Source: Space2Grow research

Key Recommendations

Children

- Develop interactive resources / tools that enable children to self assess their digital risk exposure.
- Aggregate and provide learning tools for easy access and use by primary stakeholders: children, parents and educators.
- Create and promote safe spaces for children at home and in schools where they can share their experiences and learn about safety.
- Building capacities of young leaders who advocate for digital safety and support their peers

Law Enforcement and Policy Makers

- Organising state-level multi-stakeholder round tables and establish an awareness and redressal chatbot managed by the Women and Child Development (WCD) department.
- In addition, establish a one-stop online redressal centre where individuals, especially children, can easily report incidents and seek immediate support.
- Explore partnership with the cybercrime department to research and enhance the effectiveness of online reporting mechanisms. Along with this, make child counselling services a part of the redressal process of the cybercrime unit.
- Develop SOPs and guidelines to enhance reporting and redressal practices for law enforcement (LE), accompanied by user-friendly handbooks and training resources for LE personnel.

Parents / Teachers

- Mass awareness campaigns in collaboration with government entities such as MeitY and MWCD, targeting first responders to raise awareness and promote online safety.
- Aggregate learning resources and create an easy-to-use tool that can be integrated within the existing infrastructure for teachers to help with creating awareness and redressal for children. In partnership with state governments, these apps can be internalised within state teacher training programs.

Industry

- Proactively engage with industry stakeholders such as edtech and gaming companies, and self-regulatory bodies to advocate for the development of product solutions related to age-gating and verification.
- Design a digital child safety assessment tool and compliance playbook for the technology companies that have child facing apps and products.
- Create a due diligence checklist that investors can use to evaluate companies that work with children.

Others (Mental Health Professionals, Media, etc.)

- A collaborative attempt to conduct in-depth research to explore the connections between digital risks and mental health, and develop solutions endorsed by esteemed mental health institutes.
- Initiate collaborations with media houses to spotlight the issue through impactful editorials, articles, case studies and video documentaries.

Conclusion

In summary, this research underscores the urgent need to address the safety of children in the digital space. The concerning surge in risk exposure, such as encounters with strangers, and an increased risk appetite among young internet users, coupled with a limited knowledge of reporting mechanisms and difficulty in seeking resolution, present significant challenges.

Children need knowledge, tools, and support to safely navigate the digital world, which requires collaboration between parents, educators, and digital platforms. Additionally, various stakeholders, including law enforcement, policymakers, media, mental health professionals, lawyers, and the judiciary, all play pivotal roles, as emphasised by their shared perspectives. The digital landscape will continue to evolve, and so will the challenges and concerns. What is important is the commitment to child safety as an integral component of tech innovations.

The report hence focuses on collaborative and proactive efforts that can establish a safe online environment for children, nurturing their responsible and protected online experiences.

1

Introduction

"If the internet is there, I feel like the whole world is there with me. There is no life without the internet."

– 16 year old girl, Delhi

This statement reflects children's positive perception of the internet. They depend on it. It has expanded their world beyond physical boundaries and, quite literally, connected them to the whole world. This is an undeniable truth.

The internet is a gateway to a world of endless information, entertainment, and communication. For children, it is no less than a magical space that wields immense power and influence over their lives. The World Wide Web opens doors to opportunities but also inadvertently exposes its users to risks and threats. It is a space that is necessary for a child, but also a place where they and their guardians need to be cautious.

The pervasive use of the internet has become second nature to people across the world. Data from Statista shows that 64.6% of the global population, or 5.19 billion people, are internet users. The study by Jutta Croll, 'Let's Play it Safe: Children and Youths in the Digital World', shows that even children under the age of one are exposed to the internet.

Countries such as India have seen a massive transformation in internet connectivity owing to affordable smartphones and inexpensive mobile data. The trend of children spending more time online is increasing in the region due to the internet being more accessible and affordable. They are doing so on social media, accessing EdTech content, and are spending time on gaming.

With the internet becoming a ubiquitous part of everyone's lives, Indian children are also reaching mobile maturity very early, which denotes the usage levels that they carry into adulthood. As usage levels increase, so do the associated risks. A greater share of Indian children have experienced cyberbullying and reported having private conversations with strangers online than the global average (Figure1.1). These are data points that necessitate a deep analysis and introspection into the internet usage patterns of children.

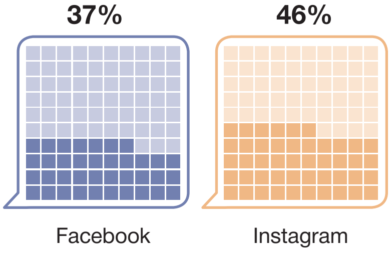
Figure 1.1: Child internet usage in India: platforms, exposure, and risks

Large user base[1]

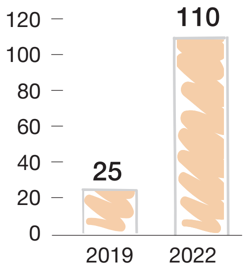
There are **66 million internet users aged 5-11 years**, constituting **15% of the total internet users** in the country

Platforms accessed by children

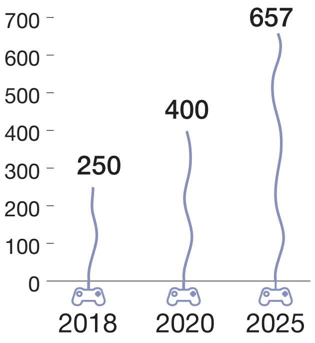
Social media[2]
Share of children in India on social media



EdTech[3]
K-12 user base (million)



Number of online gamers in India (million)[4]

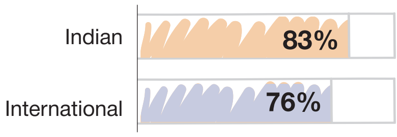


Note: Figures show all users, not just children.

Exposure and risks

Greater habit-forming[5]

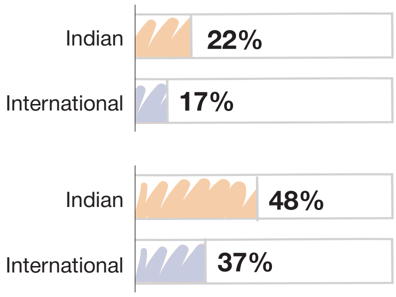
Children aged 10-14 years using smartphones



Greater incidence of risk[5]

Children experienced cyberbullying

Children had private conversations with strangers online



1. India Internet 2019: IAMAI, 2019
2. Effects of Using Mobile Phones and Other Devices with Internet Accessibility on Children: NCPCR, 2021. https://ncpcr.gov.in/uploads/165650458362bc410794e02_effect1.PDF
3. Ed Tech in India: A Turning Point: Omidyar Network India & RedSeer, 2021
4. Beyond the Tipping Point: KPMG report, 2022
5. Life Behind the Screens of Parents, Tweens, and Teens: Connected Family Study- India: McAfee, 2022. https://www.mcafee.com/content/dam/consumer/en-in/docs/reports/rp-connected-family-study-2022-india.pdf

The 2030 Agenda for Sustainable Development says that it is important to create a world in which every child grows up without being exposed to violence and exploitation, a nurturing environment that allows them to fully realise their rights and capabilities. Typically, children are nurtured within families, communities, and schools. However, with the rise of information, communication and technology (ICT), the online space has also become part of a child's environment. Thus, it is impossible to ignore the threats of violence and exploitation in this space. There is an immediate need to mitigate risks online to create safer spaces for children.

Key Research Objective

The report intends to do an in-depth exploration of the digital space from the perspective of the safety of children. This report aims to understand children's online experiences, including the risks they face and how they protect themselves. For this purpose, the responses of key stakeholders—parents, teachers, law enforcement, judiciary, mental health professionals and others—who ensure the digital safety of children and form their ecosystem were taken.

Box 1.1: Study objectives

1.

To understand existing and changing trends of online behaviour patterns of children in India across age groups, gender and location.

2.

To analyse the perceptions of key stakeholders: children, parents and caregivers, teachers, industry, and government institutions.

3.

To understand and assess the vulnerabilities amongst children vis-a-vis platforms, institutions, and other spaces that provide online services for them.

4.

To understand existing tools for self-assessment of vulnerability of children and design appropriate tools for self-tests and self-remedy.

5.

To understand existing solutions, including laws, best practices, gaps and challenges to provide recommendations for stakeholders.

The Evolving World of Cyber Crimes Against Children

The risks that children face on the internet can be categorised into three groups, which are as follows:

Content

Potentially harmful or illegal material like websites promoting self-harm, hate speech, pornography, and violence.

Conduct

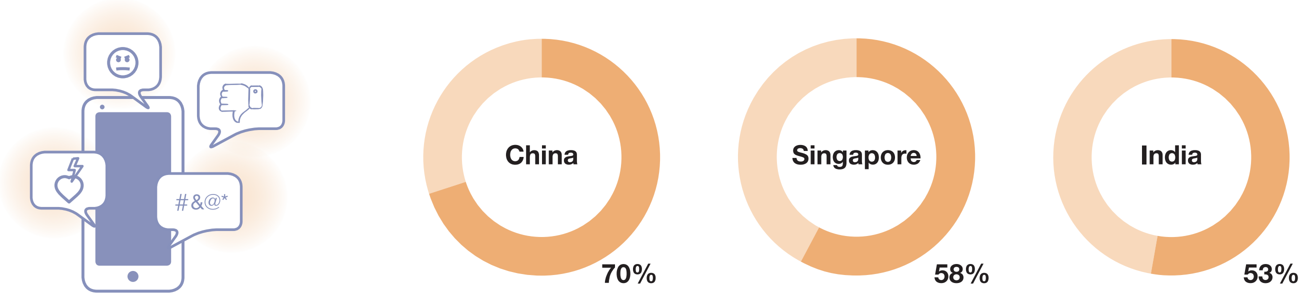
Children's internet habits, such as gaming and social interactions, can lead to addiction, cyberbullying, fraud, and privacy issues.

Interaction

There are risks involved in communicating with strangers online, such as online grooming and encountering abusive individuals.

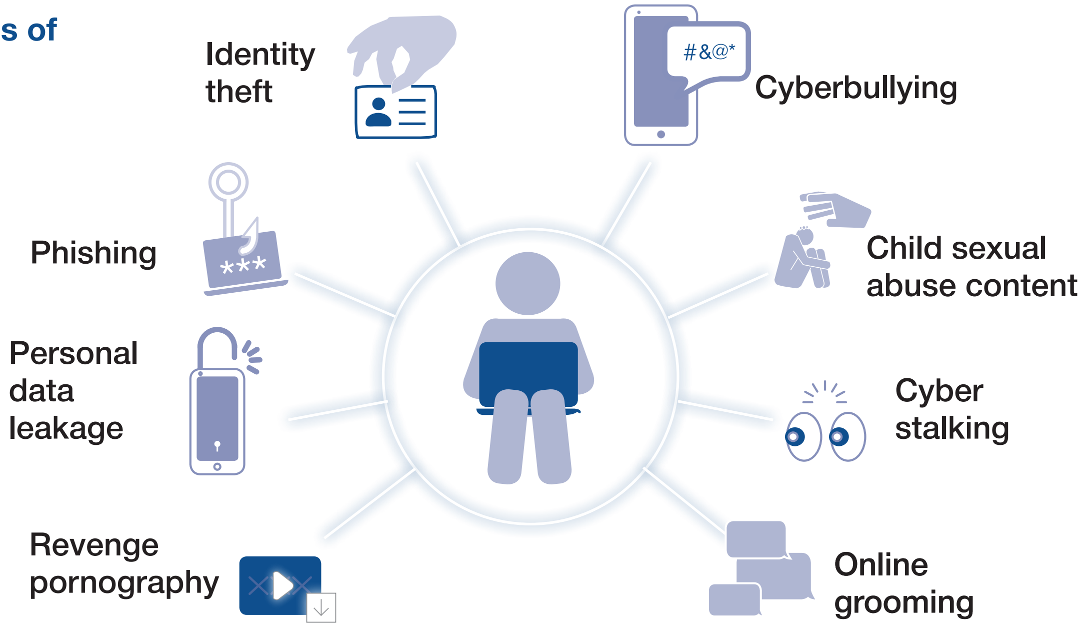
These risks can manifest in the form of several serious cyber crimes against children. A global survey conducted by UNESCO on cyberbullying of over 7,600 children and youth (aged 8–17 years old) in 25 countries revealed that the highest rate of cyberbullying is in Asia (Figure 1.2).

Figure 1.2: Asia has the highest rate of cyberbullying



Survey of 7,600 children and youth (aged 8–17 years old) in 25 countries
Source: UNESCO

Figure 1.3: Types of digital risks

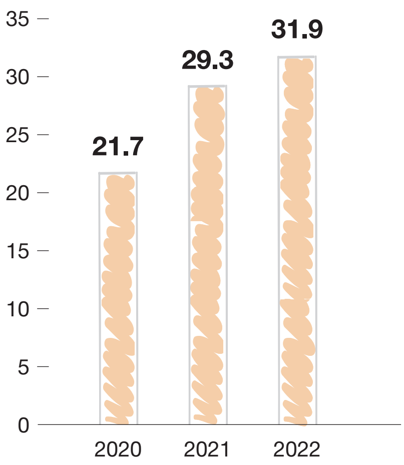


Source: Space2Grow research

The rapid evolution of technology and the increasingly widespread use of the internet have changed the face of child digital harms globally. Assessing the various research, and reports on children and the risks they face online, have helped consolidate and define 'Digital Risks' for this research (Figure 1.3).

Figure 1.4: Child Sexual Abuse Material Online

Items of child abuse imagery found and removed from the internet (million)



Source: National Centre for Missing and Exploited Children (NCMEC)

In 2022 alone, the National Centre for Missing and Exploited Children (NCMEC) reported that 31.9 million items of child abuse imagery were found and removed from the internet, marking a 9% increase from the previous year (over and above 35% increase in 2021) (Figure 1.4). It is suspected that significantly more child sexual abuse material is being circulated through hidden platforms such as file-sharing networks, including peer-to-peer, and the "darknet," by offenders.

Apart from these serious crimes against children, the increasing use of the internet has several other real-world consequences. The most important one being the impact it can have on their mental health, an aspect that is often overlooked. This includes internet addiction, screen dependency disorder, anxiety, depression, substance abuse, poor academic performance, suicidal tendencies, victim shaming, loneliness, and fear of reporting. In fact, these consequences are so serious and enduring that The World Health Organization (WHO)[6] has declared gaming disorder as a disease.

[6] Classification of Gaming Disorder: World Health Organisation 6. https://www.who.int/standards/classifications/frequently-asked-questions/gaming-disorder#:~:text=Gaming%20disorder%20is%20defined%20in,the%20extent%20that%20gaming%20takes

What are the existing frameworks to mitigate online risks for children?

Against the backdrop of the ever-evolving threats to children's digital safety, measures are being taken globally to combat these issues. Significant progress has been made through international regulatory frameworks and accords. Taking into account the new and emerging threats, these global frameworks have also evolved to offer effective tools and regulations to combat these challenges, focusing on creating safer online spaces, fostering digital empowerment and literacy, and enabling active child participation in digital activities. The efforts span from global frameworks, like the 1990 Convention on the Rights of the Child, to more localised strategies like the European Commission's Better Internet for Kids initiative.

Global Safety and Compliance Framework

International Instruments (Europe/US):

- Convention on the Rights of the Child (1989) sets international standards for children's rights, covering various aspects like survival, development, and protection from exploitation.
- Optional Protocol (OPSC 2000) focuses on the criminalisation of Sale of Children, Child Prostitution, and Child Pornography.
- Palermo Protocol (2000) aims to combat human trafficking, including that of children.
- Council of Europe Convention on Cybercrime (2001) tackles crimes committed via the internet and other networks, promoting international cooperation.
- Council of Europe Convention (2007) is dedicated to preventing sexual offences against children and prosecuting perpetrators. COPPA (1998) in the US restricts the collection of personal information from children under the age of 13 by online services.
- Online Safety Bill -2022, UK, aims to regulate digital services to tackle harmful content, with a strong focus on protecting children online.

California Law (2022):

This legislation, dubbed a "first-of-its-kind social media transparency measure", aims to shield Californians from online hate and disinformation. Under this law, social media companies are mandated to publicly disclose their policies concerning hate speech, disinformation, harassment, and extremism on their platforms. They are also to report to the state at least twice a year about their handling of the aforementioned issues on their platforms.

Global Online Child Safety Framework (UNICEF):

Lists child online protection initiatives, departments responsible, parameters and risks.

International agencies for benchmarking of EdTech firms (ikeepsafe | EFMD Global || Holo IQ):

Evaluate edtech firms on governance, and their compliance with key indicators for benchmarking.

USE metric (World Benchmarking Alliance):

Evaluates global tech firms on child protection. It is the key international framework for providing metric indicators for assessing the safety of children in digital spaces.

India - Legal Safety Framework

India, which in the past decade has experienced mass digitisation also introduced its own measures and established legal frameworks for protecting the rights of children in digital spaces. With the evolution of technology, there have been legal changes to protect against untoward incidents, prevent misuse, and develop pathways for engagement.

IT Act of 2000 (GoI, MeitY)

It is the primary law in India dealing with cybercrime and electronic commerce.

Legal provisions

- Intermediary Guidelines Rules 2011
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Coverage of themes within the law

- Electronic governance
- Electronic Records
- Digital Signatures
- Cyber Crimes
- Penalties

Evolution of the legal framework

Amendment 2008

- Section 66A penalises "offensive messages"
- Section 69 gives power to authorities for "interception or monitoring or decryption"
- Section 67B criminalises child sexual abuse material in any electronic form

IT Rules

- Liabilities and responsibilities of intermediaries
- Prevent fake news, curb obscene information, prevent misuse of social media platforms, provide security to the users
- Grievance redressal mechanism
- Code of ethics

POCSO Act of 2012 (GoI, MWCD)

Legal framework for the protection of children from sexual offences

Coverage of themes within the law

- Sexual assault
- Sexual harassment
- Pornography

Digital Data Protection Act 2023

The primary legal provision for the protection of data privacy of individuals

Coverage of themes within the law

- Parental consent required for minor's data
- Ensure informed consent by notifying data usage purpose
- No third-party data sharing without consent
- Prohibition on tracking and monitoring children's behavior

Support Services for Children

- In addition to the above, the National Commission for Protection of Child Rights (NCPCR) has also issued guidelines for online safety in schools and a portal called e-baalnidaan for registering complaints.

- National cybercrime portal for reporting and helpline number: 1930.

The research data was analysed, and documented in the absence of the ACT

A deep dive into the complexities of the digital safety of children reveals the sobering reality. By the time one threat is understood and a way is found to protect the children, another threat pops up.

While, along with governments, industry and civil society have also made strides in the attempt to protect children online, the responses so far are disaggregated, and a more in-depth understanding of the changing behaviours and norms is needed.

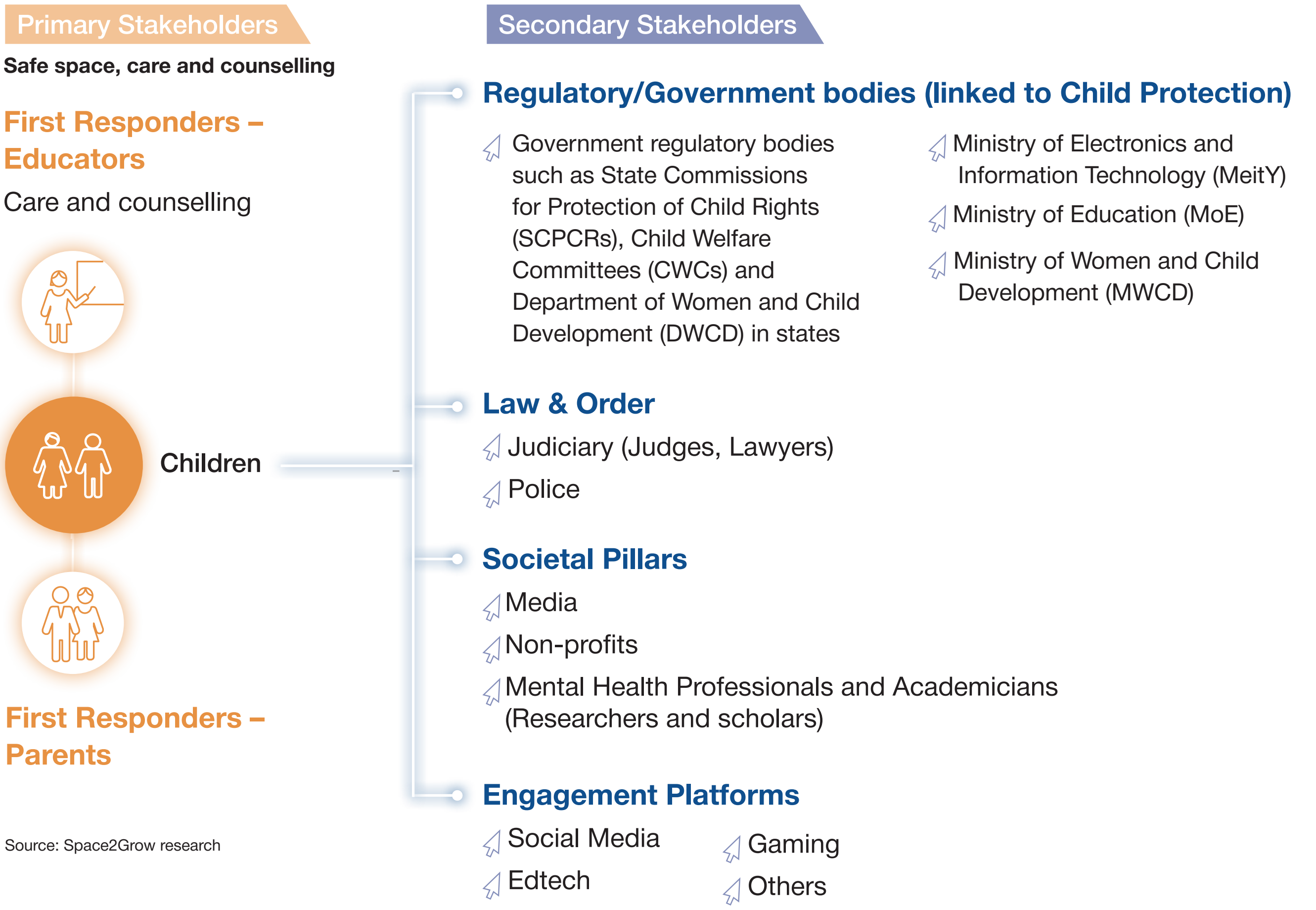
This realisation highlighted that it is important, and urgent, to initiate this research into 360-degree perspectives on the digital safety of children in India.

2

Research Methodology

The digital environment is complex and rapidly evolving. There are numerous individuals, organisations, and entities that are creating, managing, and regulating it. They form the complex ecosystem through which a child lives, learns, and interacts in the digital world (Figure 2.1).

Figure 2.1: The stakeholder landscape



Primary Stakeholders

Safe space, care and counselling

First Responders – Educators

Care and counselling

Children

First Responders – Parents

Secondary Stakeholders

Regulatory/Government bodies (linked to Child Protection)

- Government regulatory bodies such as State Commissions for Protection of Child Rights (SCPCRs), Child Welfare Committees (CWCs) and Department of Women and Child Development (DWCD) in states
- Ministry of Electronics and Information Technology (MeitY)
- Ministry of Education (MoE)
- Ministry of Women and Child Development (MWCD)

Law & Order

- Judiciary (Judges, Lawyers)
- Police

Societal Pillars

- Media
- Non-profits
- Mental Health Professionals and Academicians (Researchers and scholars)

Engagement Platforms

- Social Media
- Gaming
- Edtech
- Others

Source: Space2Grow research

Methodology

We employed a stratified purposive and snowball sampling design to interview school-going children in different age groups. This includes children from urban and rural settings, attending government and private schools. The age groups interviewed are 9-12-year-olds (preteens) and 13-18-year-olds (teens). The chosen research locations were Bengaluru and Delhi (urban Tier 1 cities) and two rural areas: Raisen district in Madhya Pradesh and the Tumkur district in Karnataka (Refer Figure ES1).

The methodology incorporated a combination of surveys, structured interviews, and qualitative approaches. In addition to primary research, secondary research tools were utilised, including findings from previous studies and work conducted by other organisations on digital safety. Relevant insights from Space2Grow's previous work in this area were also taken into consideration (Refer Appendix 5).

Data Collection

One-on-one in-person interviews and focus group discussions were conducted with children, parents, and teachers in the field. Stakeholder groups, including the community, government, and industry stakeholders, were also engaged through structured and semi-structured interviews, as well as focus group discussions.

URBKAP Analysis

The data analysis process entailed identifying emerging themes within the findings and conducting additional research to explore various aspects of digital safety impacting children, including risks, behaviour, and knowledge. This data was then used to develop a comprehensive URBKAP framework, which thoroughly examines the information. The framework centres around three vulnerability factors: internet usage, risk exposure, and online behaviour. It also encompasses three protection factors: knowledge, attitude, and practice (Figure ES2 in Executive Summary).

Note: The stratified purposive methodology uses survey respondents that have been specifically chosen based on a set of predetermined characteristics which include the use of the internet, being in school (government/private), and specific age groups. Snowball sampling is another such non-probability-based methodology that uses referrals from existing respondents to recruit newer respondents for research purposes.

3

Findings Across URBKAP: Usage, Risks & Behaviour

1. Usage

In this study, usage refers to how children connect to the internet, including the devices they use and the purpose behind using them.

Vulnerability
Factors such as internet usage, risks, and behaviour online collectively define the vulnerability of children in online spaces. These, whether considered individually or in combination, contribute to the vulnerability experienced by children online.

Children's time spent using the internet

A significant percentage of children use the internet for anywhere between one to three hours per day, with 49% of children in the preteen and 44% in the teenage group.

There is a striking similarity in the internet usage patterns of rural and urban children. A majority of children in both urban (72%) and rural (77%) areas spend between 1 to 5 hours daily on the internet. Additionally, there is a prevailing trend of gender neutrality in terms of usage. Of the children surveyed, 77% of boys and 72% of girls use the internet for 1-5 hours per day.

However, findings reveal that the time spent online increases with age as they transition from preteen to teens. The research shows that 19% of preteens spend 3-5 hours online, and over 40% of teenagers fall within the same time range when accessing the internet.

Who owns the devices used by children?

A significant majority of preteen children rely on their parents' devices to access the internet. The number of children who own devices increases with age. Among preteens, 21% own their own devices, compared to 50% among teenagers. Between rural and urban areas, 48% of urban children and 32% of rural children have their own devices.

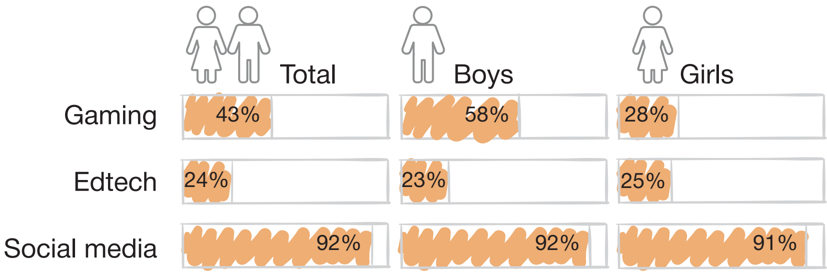
Preteens use their parents'/siblings' devices mostly across rural and urban locations. These devices have no restrictions for children and are breeding grounds for all kinds of unchecked content and perpetrator interactions. Although this usage of the parents' phones may appear safe due to the device's protection, assuming there are device safety apps installed on their phones, it actually increases the risk of unsupervised interaction between children and adults on various platforms. It also opens up access to unfiltered and inappropriate content.

> "I talk to my father's friends on his gaming account. His friends also talk to me on WhatsApp sometimes. I am not sure if he is aware of my conversations. I haven't spoken with him on this."
>
> —9-year-old girl,
> out-of-school, Delhi

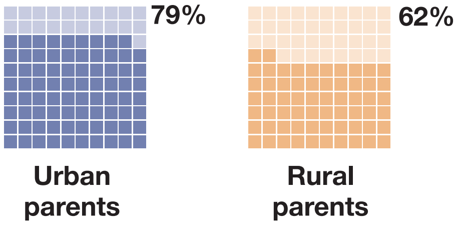
Usage pattern across platforms

The vast majority of children, almost 92% of them, are active social media users. Here, 43% are on gaming platforms and 24% of the children surveyed access edtech platforms (Figure 3.1). Children's participation on social media and gaming platforms is almost entirely influenced by peers and siblings, whereas joining edtech platforms is almost entirely influenced by parents and teachers.

Figure 3.1: Usage across platforms



Parents who know their child's usage of social media



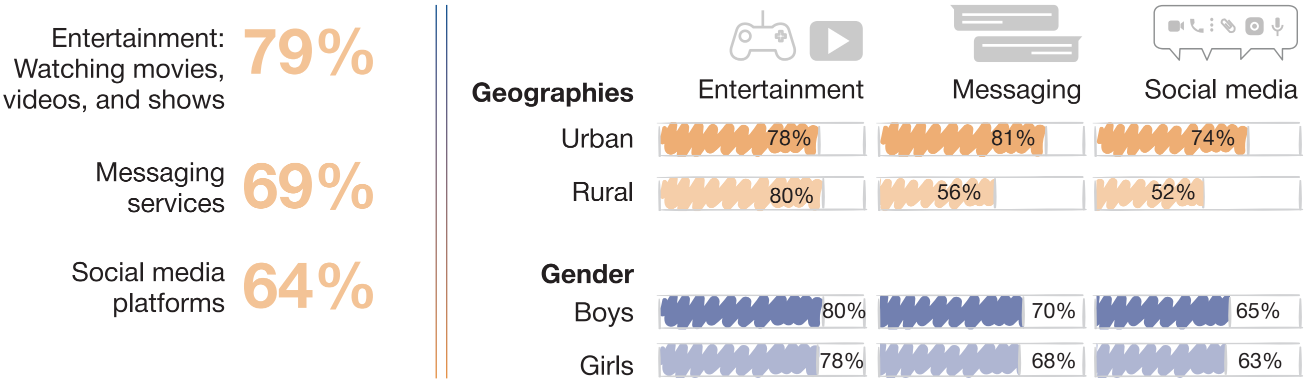
Source: Space2Grow research

Notably, of the children surveyed, 46% joined social media and 58% joined gaming platforms as preteens, despite the guidelines set by social media companies of a minimum age requirement of 13 years. This includes access to games that are not labelled as appropriate for preteens. Additionally, there is a higher prevalence of urban children joining digital platforms as preteens compared to their rural counterparts. With urban preteens, 50% of them were on social media and 62% on gaming platforms, while the distribution among the rural children was 41% social media and 54% gaming.

What are children using the internet for?

Children primarily use the internet for three reasons: entertainment, messaging, and social media. Entertainment (watching movies, videos, and shows) is the top usage and a primary online activity for 79% of children, making it the most popular. Messaging services such as WhatsApp and Messenger rank as the second most common activity, with 69% of children using them frequently. Social media platforms such as Facebook, Instagram, and Snapchat take the third place, accounting for 64% of their online activities. Online learning ranks seventh in the list with 33% of children using the internet for learning. Other uses include school projects, general browsing and online gaming (Figure 3.2).

Figure 3.2: Children and the Internet



Source: Space2Grow research

2. Risk

Risk and the term ‘risk appetite’ refer to the level of willingness of children to engage in online activities that could potentially expose them to harm or danger. Various factors may influence a child’s risk appetite in the digital space, such as the point of access to the internet, interactions with strangers, and experience of digital risk across platforms.

What is the child’s point of access?

A child can access the internet, either through private internet connections at home/school or through public Wi-Fi networks available in shared spaces. Public Wi-Fi, in particular, has been a cause of concern due to the lack of privacy and security. These networks expose children to risks such as theft of sensitive information through hacking, making them more vulnerable. In fact, rogue public Wi-Fi access points can be set up by attackers to mimic legitimate networks, tricking users into connecting to them and divulging their information[1].

According to the research conducted by Space2Grow, 23% of teenagers use public Wi-Fi connections (28% of urban children and 13% of rural children) to access the internet.

Children who participated in the focussed group discussions (FGDs) lacked an understanding of the risks of using public Wi-Fi or logging in to a public computer at cybercafes. However, the children indicated they use public access points when they are away from the home network.

Do children interact with strangers online?

During the FGDs, both parents and children indicated awareness of the concept of “stranger danger”. However, data from children’s interviews indicate children are not particularly concerned about interacting with strangers and do not perceive it as a significant threat, although some gender and location-based differences exist. Children of different ages and backgrounds frequently receive online messages from strangers. The incidence is higher for teens on multiplayer games. Urban boys have a higher likelihood of interacting with strangers online, compared to rural children and girls on gaming, social media, and edtech platforms (Figure 3.3).

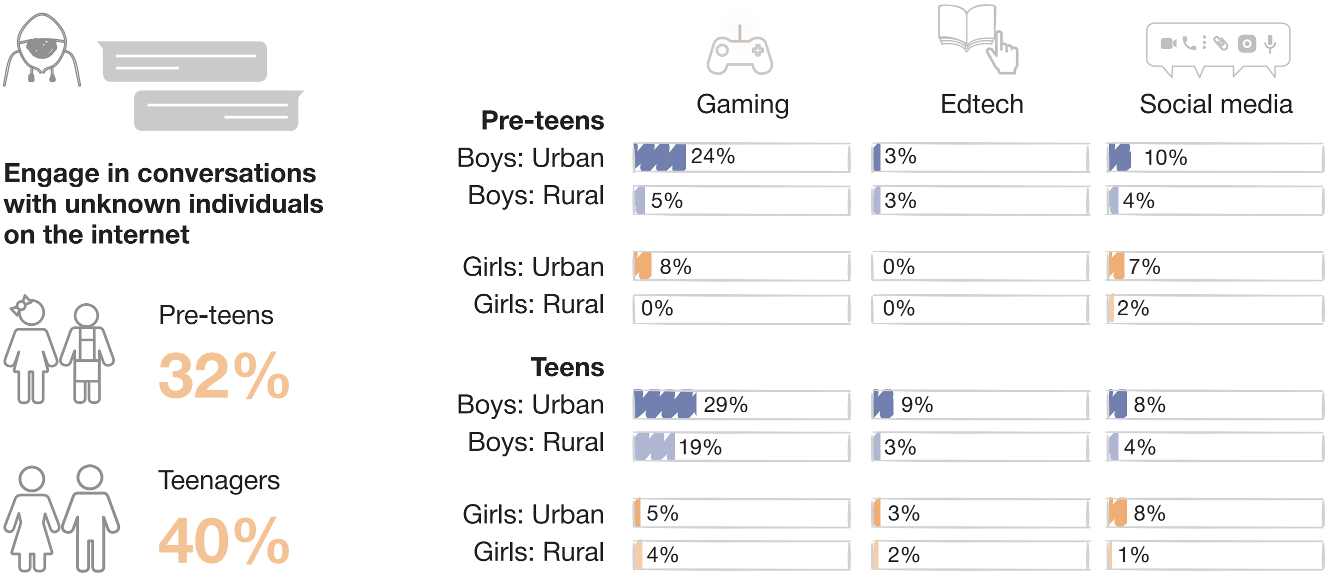
The chairperson of a Child Welfare Committee (CWC) shared a case of a girl who fell victim to blackmail. The girl met a boy online and formed a relationship. This inevitably led to in-person meetings when the boy clicked explicit pictures of the girl. Later, he threatened to post them online and extorted her for money. While the CWC was quick to take action as per the Juvenile Justice Act, the chairperson shared it was too little too late. The impact of the event affected the mental health of the girl.

[1] Choi, Carpenter & Ko (2021)

Note: Considering the age of pre-teens and in adherence to ethical guidelines, they were not asked about the possibility of meeting strangers in person after online interactions. This approach aimed to protect them from having to be involved in or discuss such matters.

One striking finding is that 60% of teenagers who interacted with strangers online have physically met with them, of which 34% did not inform a primary stakeholder or others about the meeting. Of the teenagers that met with strangers in person, 58% (61% boys, and 52% girls) admitted to having no knowledge of digital safety before doing so. Such physical meetings may lead to potentially unsafe experiences, warranting a need for increased awareness and sensitisation among both teenagers and their guardians.

Figure 3.3: Children and interaction with strangers online



Note: The aggregate figures represent the instances of children encountering strangers across various platforms, encompassing multiple platforms selected by children during the interview. The specific breakdown of encounters with strangers on the listed platform is exclusive to that platform.

Source: Space2Grow research

The EU Kids Online (2011) research report that surveyed **25,142 children** on online safety revealed that **9% of children** have met an online acquaintance in person. Of all the children surveyed, **one in nine children encountered risks** or felt bothered by such a meeting,

To delve deeper into this topic, children were presented with a hypothetical scenario involving meeting a stranger at a cafe and subsequently finding themselves in an uncomfortable situation. When asked how they would handle it, the majority of children indicated they would make an excuse to leave, send a text for assistance, or seek help from the cafe staff. The children were then asked if they would still be open to meeting a stranger after previously experiencing an uncomfortable situation. To this, 33% of teenagers (37% boys and 29% girls) expressed a willingness to build friendships with strangers once again. Further, 12% of teens and 18% of pre-teens said they open unknown links out of curiosity.

Children's Experiences of Digital Risks

Gaming: 54% of children have faced digital risks on gaming platforms (53% of boys and 57% of girls faced digital risks). The top three types of digital risks faced on gaming platforms are grooming, cyberstalking, and cyberbullying. Children expressed that receiving abusive and threatening messages during games is quite common for them.

Social media: About 46% of users joined social media as preteens and 38% of children (teens and preteens) have faced digital risks on the platform (39% of boys and 37% of girls faced digital risks). The top three types of digital risks faced on social media platforms are phishing, identity theft, and stalking.

Edtech: Edtech has evidenced that 26% of children face digital risks (20% of boys and 32% of girls). The top three types of digital risk faced in edtech platforms are cyber stalking, phishing, and bullying.

Note: Each child was explained different types of digital risks[2] before the start of the interview.

Box 3.1: Cases shared in the course of the survey

Social Media

"I once got into a WhatsApp conversation with a 25-year-old man who worked as the driver at my place of employment. Over time, he persuaded me to engage in intimate conversations and began emotionally manipulating me to meet him privately. When this happened, I felt afraid and promptly reported the situation to my employer."

—16-year-old girl, New Delhi

Gaming

"XYE (name changed) is a game where people can communicate with each other. Since everyone is a stranger, conversations can turn abusive."

—15-year-old boy, Bengaluru

"Giving commands such as 'Murder', 'Shoot at head level!' to each other is very common and the children consider it to be 'cool'."

—17-year-old boy, Bengaluru

Edtech

"Once, a girl from my class played a prank on me. So, in response, my friends and I bullied her online until she apologised. It made me popular among my classmates, I gained acceptance and my friends and peers thought of me as 'cool'."

—15-year-old boy, New Delhi

Cyberbullying emerged as a recognised risk among most respondents, with many having either personally experienced it or know a friend who had been a victim of online bullying.

[2] Digital Risks: Any risk/harm/threat or abuse faced by a child online and includes child sexual abuse content, phishing, identity theft, grooming, cyberbullying, cyberstalking, etc. Refer to the glossary in Appendix 1

3. Behaviour Online

How do children prefer to socialise?

Children were presented with a hypothetical scenario to gauge their response. The children were asked how they would react if a friend contacted them, expressing that they were feeling unwell. In that scenario, only 32% of the children indicated a preference for meeting their friends in person, while 63% preferred to connect digitally through calls or messages to check on their friends. The preference for interacting on messaging platforms rather than through calls or physical visits was evident in the interactions.

How Do Children Behave Online?

Posting and sharing online leaves a digital footprint in the form of photos and personal information and is driven by the desire for social validation. It is a behaviour that carries risks of information being accessed by malicious actors, with the added challenge of not being able to completely remove the information once it is posted. This means that all the data remains on the internet forever and can be misused (Appendix 4[3,4]). It was evident that 88% of teens and 24% of preteens post pictures and personal information without adequate knowledge of the potential consequences.

Teenagers on social media, irrespective of gender, often exhibit the habit of regularly checking their likes and comments. The pressure of gaining followers and receiving likes is also impacting children. 31% of children stated that they are adversely affected when they don't receive positive comments on social media.

The mental health practitioners we interviewed expressed significant concerns regarding the growing impact of internet validation on children, which is also increasingly becoming a leading cause of anxiety and depression.

Figure 3.4: Children and Social Interaction

Prefer in-person interactions
32%

Prefer to connect digitally
63%

Figure 3.5: Regularly Post Online

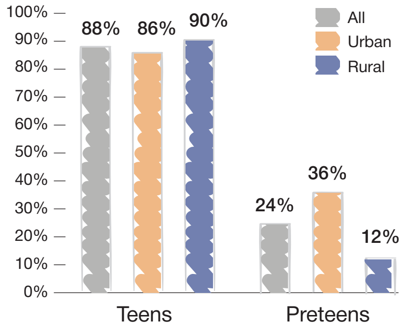


Figure 3.6: Pressure of followers and likes

31%	32%	29%
Children	Teens	Preteens

Source: Space2Grow research

[3] Social Media Use in Emerging Adulthood Berryman (2014)

[4] Children's Digital Footprint Management Strategies Buchanan et al. (2015)

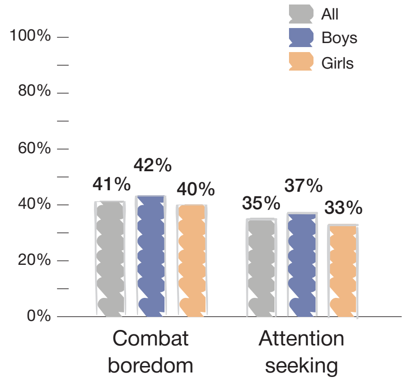
Key motivators for teens to be online

The question "What were the motivations behind being online?" was posed to the teenage respondents. The responses offer valuable insight into the motivations driving children's digital exploration. Key motivators to be online are boredom (41%), and social validation or the desire to be known, liked, and followed (35%), and this does not differ much for boys and girls and within urban and rural contexts (Figure 3.7). These factors play a significant role in their online engagement and expose them to potential risks.

How do children react to limited internet access?

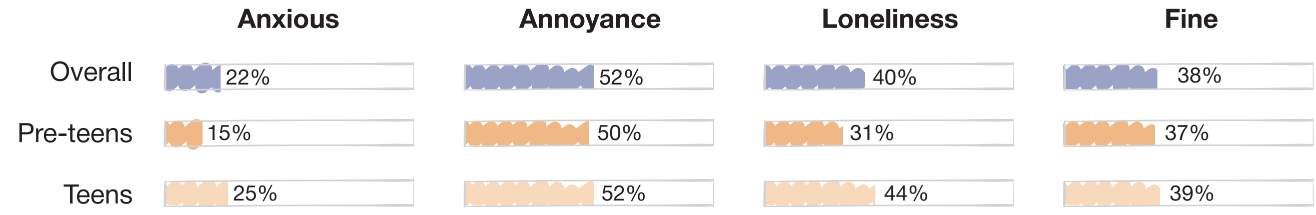
Children appear to have a sense of deep connection to the digital world. When asked about how they would react to staying away from the internet for a few days, the responses from the preteen group varied. Around 50% mentioned that they would feel annoyed, 31% expressed a sense of loneliness, 37% stated that they would be fine, and 15% reported feeling anxious. In contrast, the responses from teenagers indicated a higher level of anxiety and loneliness (Figure 3.8). It is worth noting that rural children, in comparison to their urban counterparts, mentioned lower levels of loneliness and anxiety in relation to staying away from the internet.

Figure 3.7: Key motivators to be online



Source: Space2Grow research

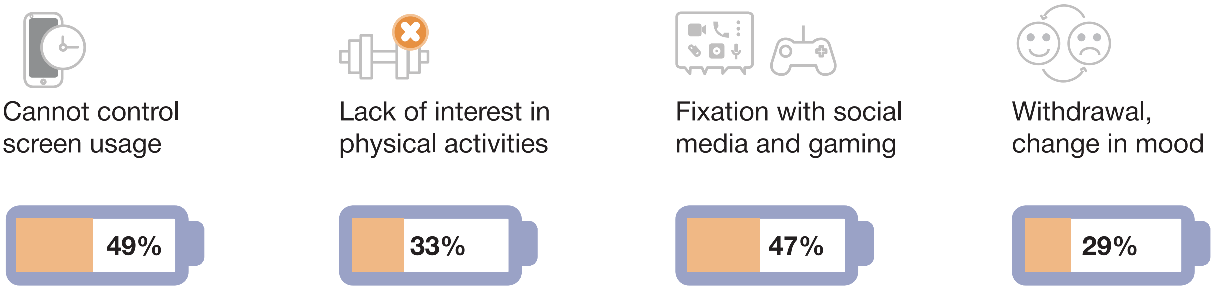
Figure 3.8: Response to limited Internet access



Source: Space2Grow research

Parents have come to realise this as well, with about 39% of them stating that they have noticed various signs of digital addiction. Some of the signs include the child's inability to control their screen usage, decreased interest in physical activities, excessive fixation with social media and gaming (such as posting about daily activities and being overly concerned about likes, and comments), and noticeable changes in mood when access to the internet is restricted or withdrawn (Figure 3.9).

Figure 3.9: Signs of digital addiction as per parents



Source: Space2Grow research

Box 3.2: Some responses from children and other stakeholders

"I do not feel good when I do not have the phone with me. It makes me enraged. I cannot live without my phone."

- 17 years, Male, Delhi

"If I do not use the internet, I will feel lonely and I will not be able to talk to my friends."

14 years, Female, Raisen (MP)

"If I don't use my mobile for even a day, I become very irritable and don't feel like talking to anyone at home."

- 17 years, Female, Raisen (MP)

"Social anxiety and depression are prominent among children. They are having difficulty making new friends offline."

- Secondary stakeholder
Mental health professional

"Removing personal information shared on platforms is a huge challenge as it is stored on the respective platforms, and we can never be sure if it is fully removed."

- Secondary stakeholder
DCP Cybercrime

The statements in Box 3.2 demonstrate the extent to which children's sense of identity and self-worth is intertwined with their electronic devices. Phrases such as "Mobile is my life" and "This is the only tool to make me happy" illustrate their belief that these devices are more than just means of communication and entertainment. The devices appear to be fundamental to these children's identity and overall happiness.

4

Findings Across: URBKAP: Knowledge, Attitude, Practice

1. Knowledge

Knowledge refers to the level of awareness, understanding, and familiarity children acquire through various means, such as attending training sessions or engaging in conversations with parents or trusted adults about potential risks and safety measures in the digital domain. For first responders, this encompasses the awareness gained through a single training attended.

Protection

The factors related to children's knowledge, attitude, and behaviour in the face of vulnerabilities collectively influence their capacity to protect themselves online. This is because possessing knowledge about digital safety, combined with heightened awareness, brings a shift in attitudes toward digital vulnerabilities. These altered attitudes, in turn, allow them to take suitable actions when confronted with threats.

How aware are children?

Only 30% of the children surveyed exhibit awareness of online safety (31% boys and 28% girls, with no difference in urban and rural) attributed to either their participation in digital safety training or through discussions with parents/teachers.

When faced with digital risks, 68% of preteens and 39% of teens admitted to not knowing what to do and how to handle such situations. Within this, a marginally higher percentage of girls expressed a lack of awareness compared to boys.

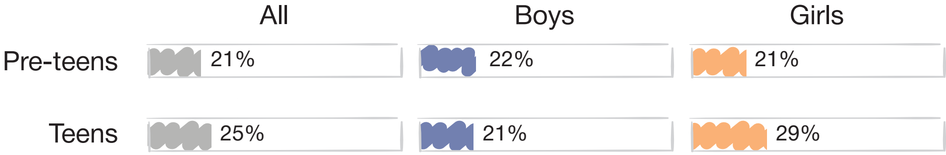
Provision of formal training to children is very rare, with a mere 16% having received any form of training at all. Among those who received training, the primary source was their school, followed by other sources, such as NGOs or NCC workshops. When it comes to discussing cyber safety with children, there is a significant lack of communication across all age groups.

Only 21% of preteens have received parental guidance, while with teenagers, we observe a slight increase in parental discussions on the dos and don'ts, particularly among girls (29%) compared to boys (21%) (Figure 4.2).

Figure 4.1: Children's awareness of online safety

Aware of
online safety
30%

Figure 4.2: Children having discussion with parents

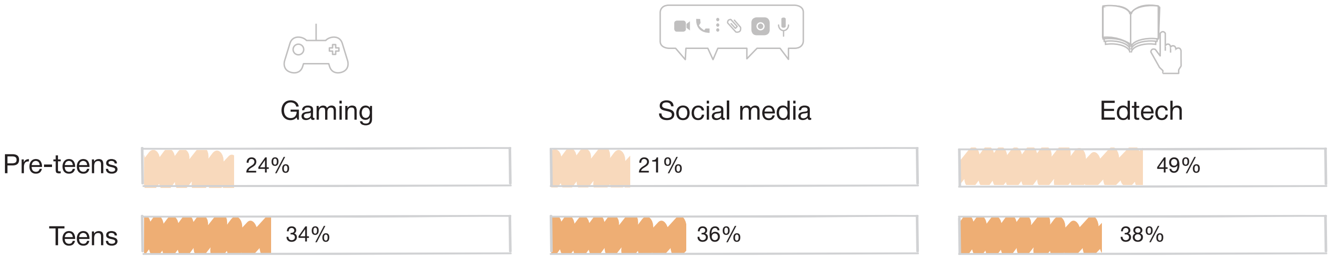


Source: Space2Grow research

Awareness of digital safety on different platforms

The data indicates the existing level of digital safety knowledge among children on the three types of platforms they frequently use. Among those active on gaming platforms, 31% are aware of digital safety protocols, while for those using educational technology, the awareness stands at 40%. Similarly, 32% of children engaging in social media have knowledge of digital safety protocols (Figure 4.3).

Figure 4.3: Aware of digital safety across platforms



Source: Space2Grow research

How aware are first responders?

According to the survey results, a high proportion of parents and teachers reported being unaware of digital safety (Figure 4.4). Among the teachers interviewed, 38% of urban teachers and 50% of rural teachers mentioned not having received any training in this area (Figure 4.5). Although parents generally believe that excessive internet use can have negative effects on children, they lack a clear understanding of the specific risks involved, and the nature and scope of these risks. In fact, 80% of urban parents are unaware of the minimum age requirements for various games.

Figure 4.4: Unaware of digital safety

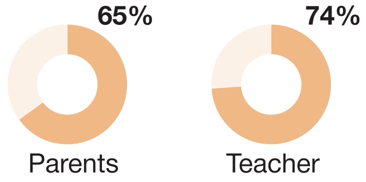
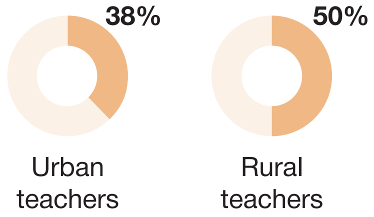


Figure 4.5: Not received any training



Source: Space2Grow research

Absence of training

Stakeholders within law enforcement also expressed low awareness regarding online abuse and crime within their teams, attributing it to insufficient training and the constantly evolving nature of such crimes. The absence of proper training for law enforcement officials makes even the small percentage of children who seek help vulnerable to risks.

2. Attitude

In this research, ‘attitude’ focuses on two main aspects: how confident children are about sharing experiences of digital risks and their preferred response when confronted with digital risks. Additionally, an important consideration is the observed shift in children’s attitudes in relation to their internet usage.

Based on the responses from children and insights shared by mental health practitioners, it is evident that the excessive use of the internet has led to a shift in attitudes, with aggressive language and behaviour becoming more normalised.

> **“I frequently use abusive language, and it’s quite common in the games we play,” stated a 16-year-old from Delhi. This statement raises concerns about the potential normalisation of aggressive language and behaviour in online spaces.**

Who is a friend or what is a ‘safe space’ for children?

Understanding Safe Space: A safe space is a person or a group of people a child can turn to. Parents, older siblings, teachers, or a counsellor, anyone can be part of the child’s safety net. A space where children won’t feel judged, criticised, or discriminated against. But will be provided shelter, help, guidance, and a sense of safety.

A safe space is especially important because, in the digital space, children face risks on every platform they engage with. Teens and preteens frequently encounter strangers online where they risk getting manipulated, harassed, abused, tricked, or even solicited.

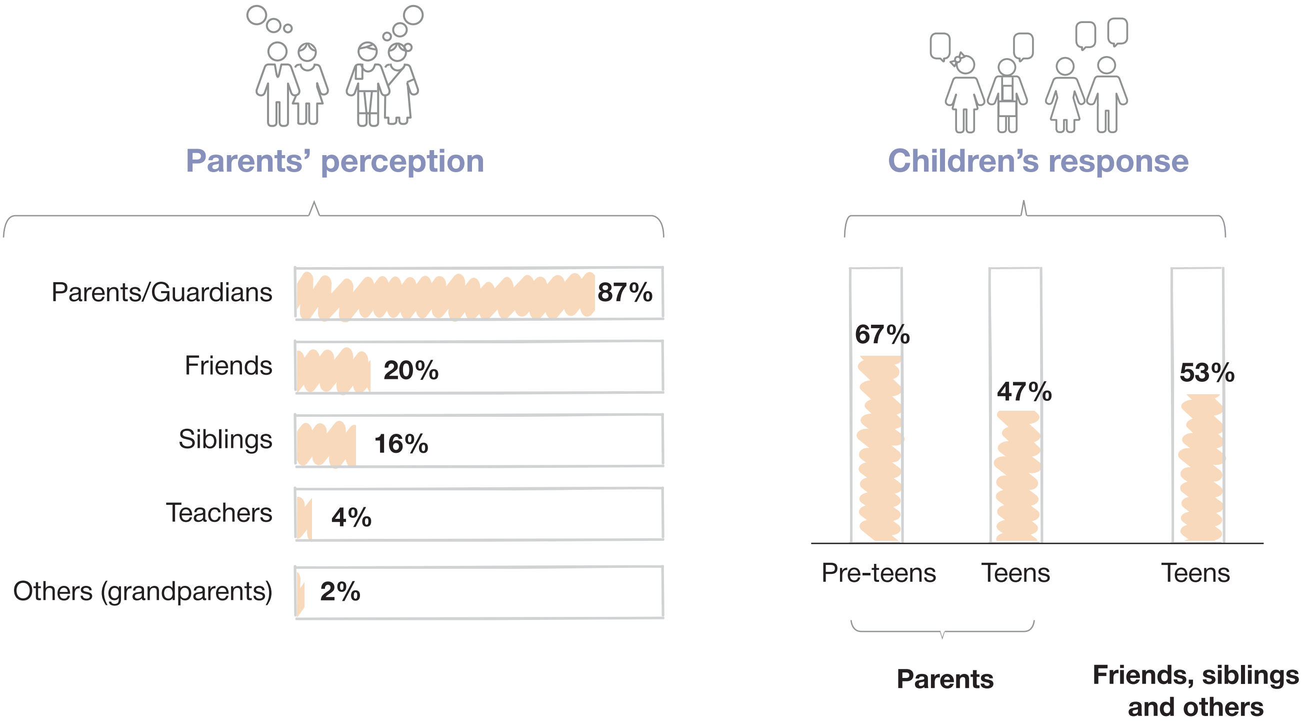
With encountering digital risks, 87% of parents believe children would feel most comfortable discussing the issue with them or their guardians.

However, the data indicates that 67% of preteens would prefer to share with parents rather than with siblings and friends in case of a situation of digital risk. The survey findings indicate a shift in preferences as children grow older. Among the teens interviewed, 53% expressed that they prefer to share situations of risk with friends, siblings or others, rather than their parents (Figure 4.6).

> "My friends and I think it is better to manage digital risk situations on our own. Involving parents or teachers often leads to unnecessary complications."
>
> —15-year-old boy, Tumkur

Moreover, the data reveals that the preference to share with parents varies based on gender: Among preteens, 70% of girls and 64% of boys prefer sharing with their parents. Likewise, more teen girls (52%) trust their parents compared to teen boys (42%) when it comes to sharing with parents.

Figure 4.6: Who a child would be comfortable sharing experiences of abuse with



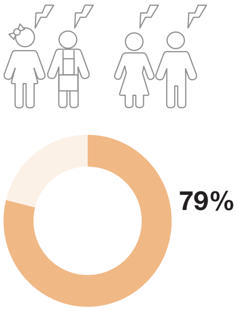
Source: Space2Grow research

What is the preferred response of children if faced with a situation of digital risk?

Overall, 79% of children prefer to handle digital risks on their own (self-intervention), which can present a challenge. This preference is influenced by the limited avenues for addressing these issues within schools and the absence of conversations about digital safety with parents. As a result, without adequate support and guidance, children may be exposed to potential risks and harm.

The responses indicate children are reluctant to share their experiences of digital risks with the police or cyber police due to feelings of intimidation regarding the legal process and concerns about the potential impact on their lifestyle. This sentiment is also supported by one of our stakeholder interviews, where a judge for the Juvenile Justice Board said that, "Children often possess an innate self-defence mechanism that leads them to conceal their online experiences and challenges from their parents. Instead, they share these issues with their peers, who might have a better understanding of their experiences with online abuse or other difficulties."

Figure 4.7: Self-intervention



79% of children prefer self-intervention

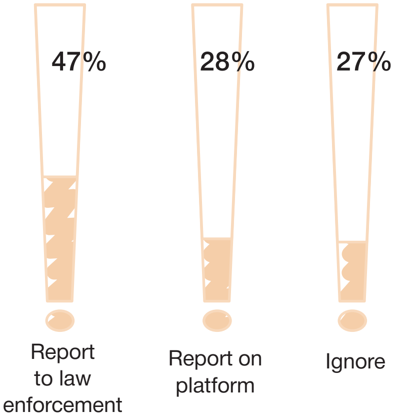
Source: Space2Grow research

Note: Self-intervention in the research refers to situations where children do not seek assistance from trusted adults or law enforcement when confronted with digital risks, and instead take actions on their own (including ignoring the risks).

What is the preferred response among parents as first responders?

Only 47% parents responded that they would report instances of digital risks to law enforcement (Figure 4.8). However, there are notable differences between the responses of urban and rural parents. Rural parents are more inclined to report to the police or cyber-police (51%) compared to urban parents (36%). Additionally, 27% of parents admitted that they are likely to ignore the experiences of digital risk altogether.

Figure 4.8: Response of parents to instances of digital risks



Source: Space2Grow research

3. Practice

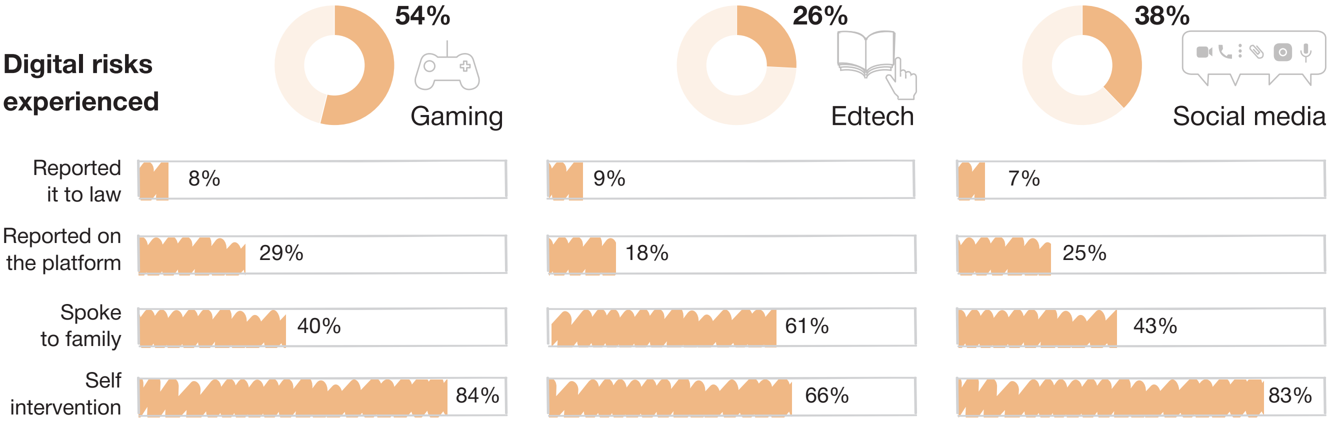
In the context of this research, 'practice' refers to the actual actions that children and caregivers take when faced with a digital risk. It is assessed by analysing what action is taken in situations of digital risks — do they report them and are their actions preventive or proactive?

What is children's actionable response to digital risks?

The data on reporting among children reveals a concerning trend: less than 10% of the children express a preference for reporting digital risks to law enforcement or helplines, while 26% would choose to report it on the platform where the incident occurred. This data suggests that children are more inclined to take matters into their own hands and engage in self-intervention when facing digital risks.

Across all three platforms — gaming, edtech, and social media — children prefer informal channels of support, such as intervening themselves, speaking to peers, and ignoring or avoiding reporting, rather than opting for formal reporting methods (Figure 4.9).

Figure 4.9: Digital risks experienced by children and their responses across platforms



Source: Space2Grow research

What measures do teachers take as first responders?

In the survey of educators, even among those who were confided in by children regarding digital risks, only 32% took proactive measures to protect the children (reporting to law enforcement and to the platform where the risk occurred). Out of this group, only 16% reported the incidents to law enforcement.

These findings align with the observations made by law enforcement officers, who have noticed a reluctance among both children and parents to report online abuse due to the fear of stigma. This apprehension can hinder them from seeking help and effectively addressing the issue. Stakeholders such as regulatory authorities, the judiciary, and legal professionals recognise that there is a stigma surrounding the reporting of cyber crimes linked to children especially linked to Sexual abuse/ Child Sexual Abuse Material.

Mediation and response by primary ecosystem

The EU Kids model divides parental mediation into two categories:
Restrictive mediation: Aimed at limiting or blocking children's access to certain types of online content or activities. Example:

- Setting parental controls and limiting screen time.
- Prohibiting certain types of online activities.

Enabling mediation: Aimed at empowering children to use the internet in a safe and responsible manner. Example:

- Discussing online risks and safety with children.
- Teaching them how to protect their personal information.
- Defining rules through dialogue and agreement.

In this study, parents were provided with a list of both restrictive and enabling techniques to regulate their child's internet usage. They were asked to indicate which measures they employed to ensure their child's safe online exploration. An overwhelming number chose restriction over enablement.

The majority of parents, that is 60%, use at least one restrictive measure to regulate their children's internet access. These measures include limiting their time spent online, allowing browsing only in the presence of parents, and restricting the location where the internet can be used. This approach was reported as the primary method of regulation by 57% of urban parents and 64% of rural parents.

A mere 3% of all parents employ enabling techniques, such as offering advice or redirecting their child's attention to other activities, to regulate their child's internet usage. On the other hand, 33% of urban parents and 35% of rural parents do not utilise any measures at all to mediate or regulate their child's internet usage.

5

Recommendations

Safeguarding children against digital risks requires a collaborative effort between multiple stakeholders. This involves meaningful dialogues to ensure that every stakeholder has a similar understanding of the prevalent risks and remedial solutions. Considering the complexities, each stakeholder has a set of responsibilities and requirements.

1. Children: Empower children by mitigating risk and enhancing their knowledge

1A Implement an interactive self-assessment tool

Acknowledging children's inclination towards self-management of online challenges and their preference for independent problem-solving rather than communicating with trusted adults is crucial to facilitating their empowerment in this context. Creating an engaging tool that enables children to self-assess their digital risks is an important step towards this. After the assessment, offering tailor-made learning materials and supportive resources will bolster their capacity for online self-protection.

1B Develop and curate age-appropriate training and awareness content

There already exists a good body of existing knowledge from which educational materials and resources can be drawn, with a special emphasis on the digital safety of teens and preteens. These resources need to be contextualised to make them engaging, culturally relevant, user-friendly, easily accessible, and customised to regional languages and different age groups. Additional steps should be taken to enhance government outreach material for children, parents, and educators with interactive and regular updates.

For example, the “Keep it Real Online” campaign by the Government of New Zealand uses creative advertising, cartoons, and textbooks to raise awareness amongst children as well as caretakers, and to equip them with the necessary knowledge and skills to ensure online safety for children.

Best practices that have had an impact in mitigating digital risks internationally and nationally should be aggregated and consolidated to make them easily accessible for children.

1C Promote safe online spaces

Creating safe spaces in schools, homes, and communities will help children share experiences, best practices, and success stories that highlight safe online behaviours and responsible digital engagement.

1D Empower champions for change

Build the capacity of young leaders who can advocate for digital safety and support their peers. Provide training and resources to empower these champions to actively promote and champion the rights to digital safety within their communities.

2. Parents / Teachers: Creating awareness amongst first responders for effective response and redressal

2A Mass Awareness Campaign

A nationwide mass awareness campaign in collaboration with government entities such as MeitY and MWCD, targeting first responders, is needed to raise awareness and promote online safety. The awareness campaign will help address the disjointed understanding of digital risks and harms amongst parents and teachers and enable better communication.

2B Aggregate learning resources for easy access

There is a need for easy-to-use tools that can be integrated into the existing infrastructure for teachers to help with creating awareness and redressal for children. The need for teachers to respond to children in given situations of digital risks and provide them with adequate support in schools makes this important. The state teacher training programs can internalise these apps in partnership with state governments.

3. Industry: Creating an accountability matrix to encourage responsibility among organisations

All organisations including start ups or non profits with a digital first-point service/access to children, ideally, should be accountable and compliant towards the digital safety of children.

3A Facilitate industry collaboration: Age-Gating

Organise roundtable discussions and collaborative efforts involving industry stakeholders to share knowledge on digital risks and deliberate on solutions to mitigate the risks including the development of solutions related to age-gating and verification, and digital safety policies. Eg: Germany has implemented age verification systems where the Kommission fur Jugendmedienschutz (Commission for Youth Media Protection) vetted and published a list of age verification vendors to ensure compliance with age restriction laws. Similar initiatives can be reviewed for efficacy, and collaborative discussions to design solutions can be initiated.

3B Develop an assessment tool and reporting mechanisms

Develop industry-specific checklists — for Edtech, Gaming, Social Media etc. — to assist organisations in self evaluating and then enhancing their products, practices, and internal policies for child-centricity and safety.

Actively engage with industry stakeholders to include online reporting options within their products, making filing cases easier, etc. The reported cases should be linked seamlessly to government reporting sites, allowing children to seek redressal directly through the platforms they use.

While international benchmarks like PEGI (European video game content rating system established to help European consumers make informed decisions) and ESRB (Entertainment Software Rating Board which helps consumers, especially parents, make informed choices about the games their families play) in the US exist for rating game age appropriateness, there’s a need for a focused matrix that assesses products based on child-centricity before they hit the market within India. Tools that are comprehensive and assess the industry’s product for children with a focus on child centricity is an essential need.

3C Investor Dialogue: Child safety due diligence for investees

Encourage investor roundtables specifically focused on edtech, gaming, and social media sectors to share knowledge on digital risks faced by children as well as proactive steps to address these. Create due diligence checklists that enable investors to assess the child safety related practices of their portfolio companies as well as new deals.

3D Promote transparency and accountability

Collaborate with government departments such as the Ministry of Electronics and Information Technology to design and establish frameworks that empower the industry to self-regulate and disclose their children's safety index. This initiative will not only enhance the branding of companies' products but also provide parents with valuable information about the safety of these products.

4. Law Enforcement and Policy Makers: Increasing access to a single window reporting and redressal

(Law Enforcement includes Police, Judiciary and Lawyers & Policy makers includes departments within government and regulatory bodies that focus on Children, digital spaces, privacy, etc.)

There is a pressing need for the creation of a one-stop centre for reporting and redressal, providing clear directions for all stakeholders involved in order to streamline the process and ensure a unified, efficient response to safeguard children in the digital realm.

4A Organise state-level multi-stakeholder round tables

To proactively address the issue, initiate roundtable discussions involving various stakeholders including government entities, industry delegates, child protection organisations, and experts to create an easy-to-use solution for redressal for children and a shared understanding of the risks. For example: A chatbot system for both awareness-building and streamlined reporting processes that are easily accessible by children through the Women and Child department. This will serve as a model for potential statewide and nationwide adoption.

4B Establish a one-stop online redressal centre

Facilitate targeted outreach through a pilot awareness campaigns in states increasing the visibility and usage of existing systems of response to educate children and parents about vital initiatives such as eBalNidan (dedicated to reporting child rights violations) and 1930 (a cybercrime helpline). Enhance support to regulatory bodies, cybercrime units, and other stakeholders to fortify these initiatives for greater effectiveness. This can be enabled through setting up dedicated technology-led units with sectoral experts to combat digital harms for children such as the ‘Keep it Real Online” campaign referred to earlier in this section.

Integrate counseling services for immediate support to child victims of cybercrimes, streamlining the reporting process and improving their overall experience.

4C Encouraging collaboration between police, judiciary, and lawyers with schools and communities

Foster partnerships and collaboration between police, judiciary, lawyers, schools, and communities to create a supportive environment that encourages open communication. This collaboration aims to break the fear of reporting cybercrimes and establish trust among children and their support networks.

Kerala has pioneered the establishment of a Counter Child Sexual Exploitation Center, a notable best practice. This innovative center is dedicated to identifying perpetrators and extending support to victims of online risks, particularly focusing on combatting Child Sexual Abuse Material (CSAM) and sexual exploitation.

4D Create law enforcement SOPs and enhance online reporting with cybercrime collaboration

Develop standard operating procedures (SOPs) and guidelines, including user-friendly handbooks and training resources, for law enforcement to enhance reporting and redressal, while also collaborating with the cybercrime department to research and enhance online reporting mechanisms.

5. Others (Mental Health Professionals, Media and Academia, etc.)

A multi-stakeholder approach is essential for providing comprehensive solutions to online safety issues. This approach should include:

5A Establish a common pool of resources

Collaborate with universities or leading mental health institutions to develop a deeper understanding of digital risks and identification of signs of risks in children for empowering first responders. Develop a complete set of resources in multiple languages for the public, including information about addiction signs, and training materials among others.

5B Conduct in-depth research

Undertake research to specifically explore the connections between digital risks and mental health. Based on the findings, develop evidence-based solutions that mitigate the negative impact of digital risks on children's mental well-being and are also endorsed by esteemed mental health institutes.

5C Collaborate with media houses

Initiate collaborations with media houses to raise awareness of the issue and encourage informed dialogue. Highlight the importance of digital risk prevention and mental health through impactful editorials, case studies, video documentaries, and articles.

5D Casework repository

Create an aggregation of information and resources from non-profit organisations, pro bono legal support providers, and helplines. This repository can be shared through universities, state governments, and central government platforms for easier access.

6

Conclusion

When asked about her reaction to the concept of digital detox, a 15-year-old from Delhi, said, “Maybe we will go back to the old ways of friendship and meet and play more”.

This statement shows that, to a certain extent, children are well aware of their dependence on the internet. They recognise the difference in building relationships with and without technology, and they value face-to-face interactions. But in the absence of viable and attractive alternative solutions, their vulnerabilities in the digital space grow. In the face of this, innovative approaches are needed to maximise their advantages and minimise their vulnerabilities in the online world.

In conclusion, the research brings attention to the persistence of vulnerabilities and digital harms experienced by children, in the digital realm. While the findings reveal a lot of similarities in usage patterns and risks faced by both urban and rural children and across genders, there are noticeable differences in usage, risks, and behaviours between teens and preteens. This emphasises the need for a strategic and targeted approach based on different age groups. Digital safety is an ongoing endeavour. Collaboration between parents, educators, law enforcement, regulators, and industry is the need of the hour to address the gaps in creating a safe digital experience for children.

The study provides substantial evidence, identifies specific areas for improvement, and empowering stakeholders to take immediate and future actions. Key barriers include insufficient communication between parents and children about digital safety, limited proactive measures in schools, the stigma surrounding reporting digital risks, lack of training and engagement, and the absence of governing frameworks for child-centric platforms.

Overall, the research highlights the low levels of awareness among first responders (parents, teachers) and the limited accessibility of secondary responders (law enforcement, mental health professionals, nonprofits, industry) to provide timely assistance to children. It emphasises the need for a cohesive effort involving multiple stakeholders to address and mitigate the risks children face. Urgency must be given to prioritising children's digital safety with measures that are easy to "access" and even easier to "click."

Addressing these challenges requires active parental engagement and enhanced collaboration among parents, schools, industry, and law enforcement. Industries with child facing apps / product need to be mindful and take conscious steps to address these risks children face on such platforms. Governments and regulatory bodies must collaborate and take a holistic view when creating policies aimed at children-focussed networking platforms.

To break the silence around reporting digital risks, it is important to implement comprehensive digital safety education, foster an environment of trust, and establish effective reporting platforms. Together, we can make the internet a safe space and valuable resource for every child.

7

Appendices

Appendix I: Glossary

These definitions are in the context of the research and based on a secondary literature review on the topic.

Child sexual abuse content: Any visual depiction of sexually explicit conduct involving a child which includes photographs, video, digital or computer-generated images that appear to depict a child

Cyberbullying: Acts of harassment such as embarrassing, taunting, insulting or threatening behaviour towards a victim by using the internet, e-mail or other electronic communication devices.

Cyberstalking: When a victim is repeatedly and persistently followed and pursued online by e-mail or other forms of electronic communication.

Identify theft: Obtaining the personal or financial information of another person for the sole purpose of assuming their identity to make transactions or to abuse someone.

Online predator/grooming: A person 'befriending' and creating an emotional bond with a child with the goal of sexually abusing them (offline, online, or both). Trust is gained through gifts, compliments, and stories to evoke empathy.

Personal data leakage: A data breach or data leak is the release of

sensitive, confidential, or protected data to an untrusted environment.
Phishing: A financial scam for attempting to acquire sensitive data, such as bank account numbers, through fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

Revenge pornography: When a former romantic partner publicly shares sexually explicit content depicting their ex, post a break-up. Said act is intended to exact revenge or humiliate the latter.

Digital detox: Refers to a period of time during which a person refrains from using digital devices such as smartphones, computers, social media platforms, and other similar digital technologies.

Edtech: Any online education platform used by children for the purpose of learning their grade-wise academics.

Gaming: Any form of gaming platform, such as websites, apps, or consoles, that children play or have access to.

Law enforcement: Includes the police, judiciary, and lawyers interviewed for this research.

Own device: Any device including smartphones, tablets, and laptops that a child has exclusive ownership of and which can be used to access the internet and use various apps.

Preteen: Respondents between the ages of 9 and 12 years.

Safe spaces: Refers to online platforms or communities that are designed to provide a safe and supportive environment for children to interact and share information without fear of harm or exploitation.

Social Media: Facebook, Instagram, WhatsApp, Discord, Snapchat, and any other social networking platform.

Stranger danger: A safety message teaching children to avoid interactions with unknown individuals, warning them to avoid interactions with strangers due to the potential threat of harm.

Teen: Respondents between the ages of 13 and 18 years.

Appendix II: Ethical Considerations

Research involving children raises a number of ethical considerations that must be carefully addressed to ensure that the rights and dignity of all participants are respected. In conducting this research, Space2Grow recognised and respected these considerations. At Space2Grow, children and their safety are always a top priority. With a wealth of professional expertise and leadership experience in child protection, the organisation is deeply committed to ensuring that children's rights and protection are at the heart of every project, program, or research. The leadership team has worked extensively with children across various fields, including livelihoods and anti-human trafficking, and this knowledge and experience are reflected in the approach taken by the entire team.

To ensure that this research was ethically compliant, we took the following steps:

- A diverse advisory board was established that reviewed the research plan and oversaw ethical considerations. All members of the data collection teams were given sensitivity training to ensure that the research was child-centred at every stage. Overall awareness of digital safety and protection was provided to the CBOs and data collection teams participating in the research.

- Research protocols were designed to protect their privacy and ensure their safety and well-being. Consent was obtained from school principals or parents/guardians before conducting interviews and surveys, with consideration given to scheduling interviews at a time and location approved by caregivers. Participants were not coerced, and they were informed of the study's purpose and their right to terminate their participation without penalty.

- Additionally, before asking children about their experiences of digital risks, the interviewers educated the children about various forms and indicators of online abuse.

- To maintain confidentiality and privacy, audio and video recordings were not used during data collection. Photos taken during interviews only showed the faces of the field staff. Personal information and names of participants were neither collected nor shared in the report or with any third parties. Specific responses of children were kept confidential, even from their parents who were interviewed for the study.

- Contact information for Space2Grow and counselling psychologists was provided to interviewees who wanted to reach out. To ensure the safety of participants, helpline numbers and cyber cell contact information were shared if any digital risks came to the team's attention during the survey.

Appendix III: Limitations

Throughout the course of our research study on children's digital safety, we diligently followed established protocols and implemented best research practices to ensure the quality and integrity of our findings. However, it is important to acknowledge that, despite our efforts, some limitations persist within our study.

Firstly, the study has a large sample size and encompasses both rural and urban locations across age groups, gender, and economic class. However, the rapidly evolving nature of the digital landscape poses a time and space limitation. The findings of this study may not be applicable in the exact same manner in the future, considering the increasing ownership of devices, faster and wider internet connectivity, and potential changes in digital practices.

Another limitation arises from the involvement of grassroots organisations in data collection. While this approach has advantages in terms of capacity building, cultural perspectives, and participant comfort, it also introduces challenges. The quality of data varied among different teams due to differences in exposure, understanding of the topic, and technical expertise. Despite some minor issues owing to the diversity of data collection teams, we have adhered to the highest quality standards and best practices.

Despite efforts to provide support and training, some teams faced difficulties in capturing effective responses, resulting in variability in data quality. To mitigate these limitations, Space2Grow conducted additional interviews and organised focus group discussions to gather supplementary data, compensating for any shortcomings in the primary data collection process.

Appendix IV: Some Key Reads

1. Children's Digital Footprint Management Strategies Buchanan et al. (2015)

Digital footprint refers to the information and data that a person leaves behind online as they use the internet and other digital technologies. This includes any personal information, photos, videos, or other content that a person shares online, as well as any online activity such as search history or social media interactions. Buchanan et al. (2015) highlight that personal information shared online can potentially be accessed by malicious actors and used for identity theft or other harmful purposes. It is important for individuals to be aware of these risks and take steps to manage their digital footprints accordingly. They argue that this can have long-term effects on children as well. The risks of digital footprints include potential negative impacts on future careers or job prospects, as well as the possibility of personal information being shared or used inappropriately. Employers and organisations are increasingly using digital footprints to verify the identity and perceived suitability of candidates for positions within their organisations.

2. Social Media Use in Emerging Adulthood Berryman (2014)

According to Berryman (2014), social media use is partially motivated by the need to fulfil social needs, including the need to be accepted. Children may use social media to connect with peers and feel a sense of belonging. The study found that there is a strong relationship between needing to belong and social media use and attachment. Additionally, people experiencing loneliness may also turn to social media for reassurance-seeking behaviours.

3. Sharenting: Children's Privacy in the Age of Social Media Steinberg (2016)

Digital footprints for the child are also created when the parents post their pictures/videos. This practice by parents is called Sharenting (Steinberg, 2016). Through sharenting, parents shape their children's digital identity long before these young people open their first email. The disclosures parents make online are sure to follow their children into adulthood, and social media and blogging have dramatically changed the landscape facing today's children as they come of age. This could lead to privacy violations, cyberbullying, and even identity theft. Additionally, the information shared by parents may be used by marketers or other third parties to target children with advertising or other content. The article argues that, unlike third parties, the people who are putting children at risk here are the people who are responsible for their protection: the parents.

4. EU Kids Online

The 'Ecological Model of Children's Online Engagement' developed by the EU Kids Online project outlines micro and macro circumstances that affect children's online involvement. It includes individual factors such as age and gender, social context such as family and peers, and broader social and cultural environment. The model provides a comprehensive understanding of how children interact with the internet and the risks and opportunities they encounter.

In this model, the child is at the centre and is influenced by individual factors like age, gender, and preferences. Children's online experiences are shaped by the meso-level influences in their immediate environment, such as their family, friends, school, and community. The macro-level elements that affect the child's digital surroundings include media coverage, governmental regulations, and the availability of digital infrastructure. These elements can have an effect on one another, as shown by the connecting arrows. The ecological model offers a framework for perceiving children's online activity and emphasises the significance of taking into account how social, environmental, and human aspects interplay when addressing children's digital well-being.

Another important contribution of the EU Kids Report has been the model analysing cross-national differences. Factors such as the market, politico-legal, cultural, and educational contexts impact the usage and determine the risk and opportunity levels. By understanding the different areas of comparative difference and the levels through which they work and interact, policymakers, educators, and parents can better understand the complex and multifaceted nature of children's online experiences.

5. Do Children Report Online Abuse?

Research suggests that children may perceive their parents' and teachers' unfamiliarity with digital safety measures as a sign that they cannot effectively address the issue, making them less likely to report online abuse (Livingstone et al., 2011). Several studies have demonstrated that children are less likely to report abuse if they believe that doing so will not result in any meaningful action (Finkelhor et al., 2000; Wolak et al., 2006). A study conducted by Wolak et al. (2006) supports this notion, revealing that only 27% of victims of online abuse reported the incident to authorities, largely due to their belief that nothing could be done to stop the abuser.

Links

5a. Risks and safety on the internet:
the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16-year-olds and their parents in 25 countries https://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet(lsero).pdf

5b. Online Victimization:
A Report on the Nation's Youth., 2000-Jun
https://eric.ed.gov/?id=ED442039

5c. Online Victimization of Youth:
Five Years Later. https://scholars.unh.edu/cgi/viewcontent.cgi?article=1053&context=ccrc

6. Other links

6a. Social media children I 38% of Indian 10-year-olds have Facebook accounts, 24% Instagram in violation of rules, finds NCPCR study https://www.timesnownews.com/technology-science/article/38-of-indian-10-year-olds-have-facebook-accounts-24-instagram-in-violation-of-rules-finds-ncpcr-study/789948#:~:text=A%20study%20commissioned%20by%20the,apex%20child%20rights%20body%20found.

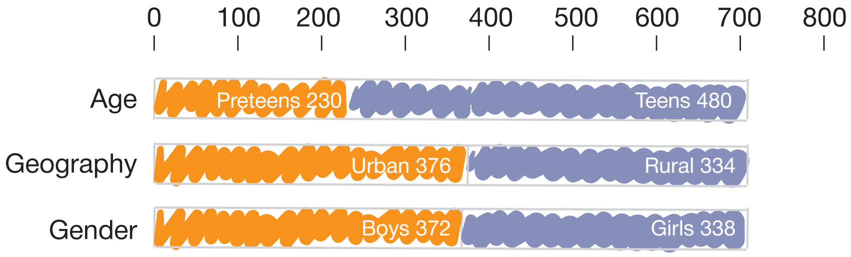
6b. https://www.missingkids.org/cybertiplinedata

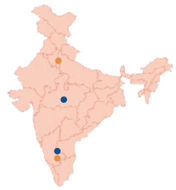
Appendix V: Research Methodology

Children

710

Additional 6FGDs (covering 90 children)





Locations

- ● Urban: Delhi, Bangalore
- ● Rural: Raisen, Tumkur

Age Groups

Preteen:

9-12

years

Teens:

13-18

years

(All children surveyed had access to the Internet)

Break-up

Caregivers - Parents / Guardians

116

Additional 4 FGDs (covering 40 parents)

Teachers

72

(from 16 schools)

Regulatory/ Law Enforcement/ Judiciary

25

Mental Health Professionals/ Media/Academia/ Industry

25

Locations

Schools - Private/ Government
Children, Teachers (Caregivers) Urban and Rural - (Outreach to Children through Government and Private Schools, covered across income levels

Community
Caregivers - Parents, Out of School Children

CWC/ SCPCR/ Education Department/ Cyber Cell/ Police/ Judges/ Lawyers
Regulatory/ Law Enforcement/ Judiciary

Pan India
Mental Health Professionals/ Media/ Academia/ Industry (EdTech/ Gaming)

Survey Tools

Survey / FGD

Children

FGDs and Structured Interviews
Caregivers - Parents / Guardians

FGDs and Structured Interviews
Teachers (Caregivers)

Semi Structured Interviews
Regulatory/ Law Enforcement/ Judiciary

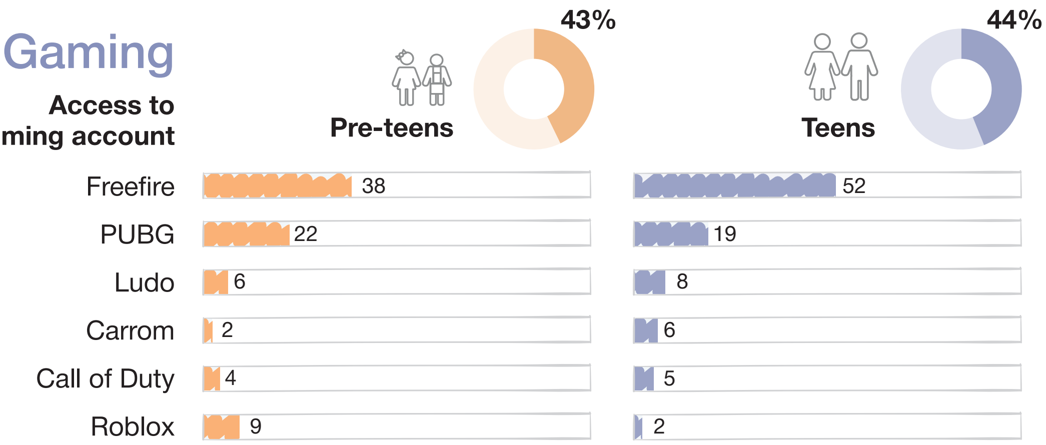
Semi Structured Interviews
Mental Health Professionals/ Media/ Academia/ Industry (EdTech/ Gaming)

Source: Space2Grow research

Appendix VI: Platforms that Children are Accessing

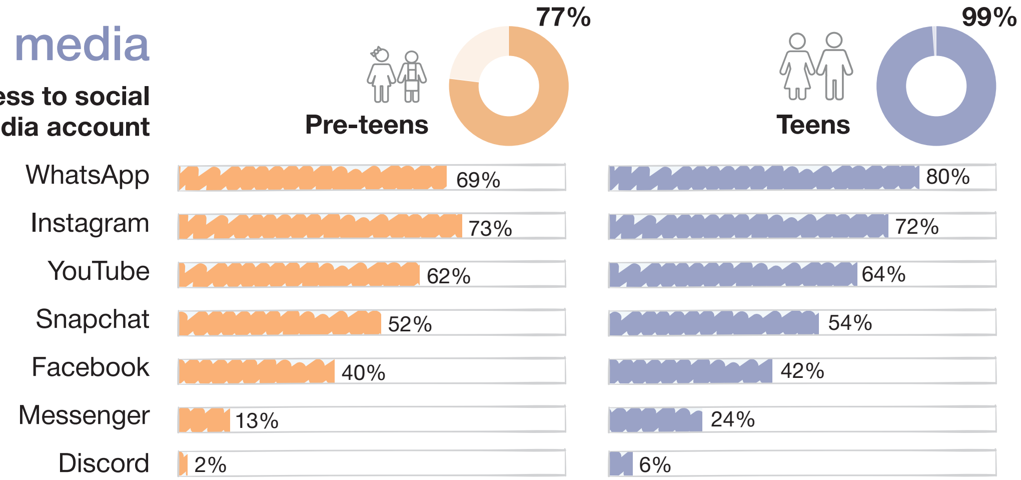
Gaming

Access to gaming account



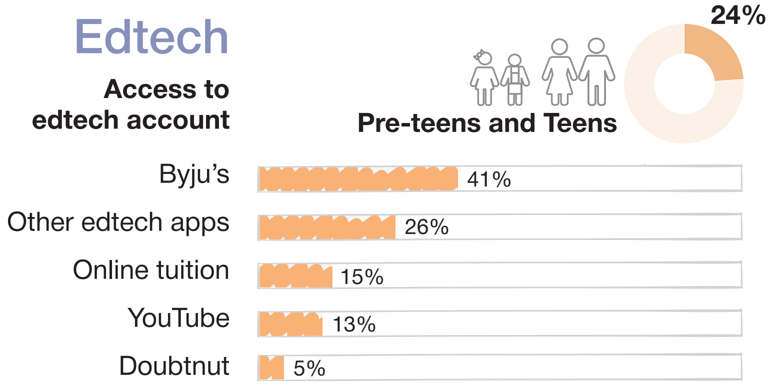
Social media

Access to social media account



Edtech

Access to edtech account



Note: The aggregate figures represent the instances of children accessing various platforms, encompassing multiple platforms selected by children during the interview.

Source: Space2Grow research