CYBER SAFETY & SECURITY

Guidelines for Parents

Version-1.1

DEVELOPMENT COMMITTEE

Chairperson

Professor Amarendra Behera, Joint Director, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Member Coordinator

Dr Angel Rathnabai, Assistant Professor, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Members

Dr Anjum Sibia, Professor and Head, Division of Educational Research (DER), NCERT, New Delhi

Dr Indu Kumar, Professor and Head, DICTandTD, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Dr Gowramma, Professor and Head, Department of Education, Regional Institute of Education, Bhubaneshwar

Mrs Simi Paruchuri, ISEA team C-DAC, Hyderabad

Mrs Soumya M, ISEA team C-DAC, Hyderabad

Mrs Nisha Dua, Mentor and Coach, Cyber Safety and SafeElearning Programs, New Delhi

Ms Himanshi Bhati , Junior Project Fellow, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Ms Kajal Yadav, Junior Project Fellow, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Ms Kunica, Junior Project Fellow, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Designer

Mr Sanjay Yadav, Graphic Artist, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Glossary of Keywords

Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

Trolling is defined as creating discord on the internet by starting quarrels or upsetting people by posting inflammatory or off-topic messages in an online community.

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

Stalking is an unwanted and/or repeated surveillance by an individual or group towards another person.

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. It typically spreads through phishing emails or by unknowingly visiting an infected website.

Virtual Private Network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so that your online actions are virtually untraceable.

Parental Controls are features which may be included in electronic gadgets (digital television, computers, laptops, mobile devices, etc.) and softwares that allow parents to restrict the access of content to their children.

Contents

In the current 'cyber age' that we are living in, we may all rightly call ourselves as citizens of the Digital World. Technology today has become pervasive, affordable and efficient. Using digital gadgets is a new norm in most of the families and households today; members of the family use digital devices for connecting with friends and family, doing online transactions, and paying taxes too. The access to technology through the convenience of digital devices is far reaching and has touched every aspect of our daily life.

In this scenario, it is evident that the current and future generation are the ones who will feel an immense impact of the technology. Today digital gadgets are used by children from a very early age, they are practically used in every sphere of activity by kids. Today children are greatly dependent on devices, quickly adapt to various mediums of digital devices and naturally learn to use smartphone applications, watch and create YouTube videos, play online digital games, use web search for learning, etc. They are the 'digital age kids' of the current generation.

Parenting in the current age is, therefore, a challenge for which one needs to be well prepared. As a parent in this digital age, one needs to have an understanding and grasp over both the positive and negative impact of technology on the child and thus have to be aware and alert. This enables them to guide the child in the right way to use the digital technology in a progressive and enabling way, at the same time, keep them at bay from the possible threats or dangers in the digital world. Parenting in the digital age requires a new adapted style of nurturing children which combines the digital awareness to their knowledge in bringing up the next generation of digitally oriented citizens who are known as netizens.

Listed below are few digital habits observed amongst the children of different ages, the impact of these practices and suggestive measures for parents to ensure digital device security and safe online experiences.

Children give a lot of importance to their **presence on social media platforms** and interact a lot with friends online.

Social media presence can leverage children outreach, communication and information. However, children of all age groups are prone to bullying, trolling, and other dangers on the internet. This can severely affect a child both emotionally and physically.

Apart from being aware and prepared to help children in such scenarios, parents should build strong and healthy bonds within the family, they should encourage children to have open conversations, share their online issues and seek guidance.

Children often use **desktop/laptop/mobiles of parents** to access the internet for various purposes like checking information to gain knowledge, playing games, etc.

The personal devices of parents contain important personal information and sensitive financial data, which can be unknowingly mishandled by children if they are not properly aware of the security threats.

Parents should be aware of the security measures to be adopted while giving access to digital devices to children. Also, they should make children aware about right practices and careful usage of digital devices.

Children **love watching videos** and are often seen to be accessing video sharing sites like YouTube.

While online videos are a good source of entertainment and information, there can be malicious links that can turn up in video sharing sites through which fraudsters can hack users' digital devices.

Parents should guide the children appropriately on the possible threats when they are online, they should be aware about these malicious links that can pop up on YouTube videos and appropriately make the children aware about the dangers of a device being hacked.

Children tend to download and *use a lot of free apps* on their mobile phones and other digital gadgets.

Free apps can infect your device with malware, ransomware and may also pose security threats such as data leakage, prone to hacking, etc.

Parents should be able to share the information related to the importance of downloading apps from authorized playstore with assistance from parents and also be alerted against security threats and privacy issues related to the usage of unsecured apps.

Children do not mind *sharing their personal information* like name, email id, address, mobile number, details of school, etc. with their online friends openly.

While online communication can build relations, sharing personal information openly can pose security-related threats like identity theft, stalking, phishing attacks, etc.

Parents should mentor the children appropriately about the dangers of sharing personal information openly online. They should be able to let the children know how it can lead to identity theft, which can be misused by fraudsters.

Children find a lot of interest in doing ***online shopping***.

While online shopping can throw open a wide range of cost-effective options, they can also pose many threats and dangers like financial theft, fake offers, unsecured/fraudulent sites, data breach, phishing attacks, malware attacks, etc.

Parents should let the children know about the threats and online financial scams that can affect them while shopping online on unsecured sites. They need to be made aware of being careful while sharing their personal and financial details.

Build Strong Parent-Child Relationships

The first step in any relationship is to build strong, healthy bonds. This will help to build trust in the child to gain the confidence to open up and seek guidance.

1. **Parent-Child Bonding:** Parents need to create an environment where the child feels comfortable and free to talk about their digital activities. The following measures can be considered by parents to bond with their child:

   🔋 **Warm, Loving Interactions:** The child must know that their parents love, support and trust them, which enables them to share their concerns regarding anything disturbing encountered by them online and to seek advice.

   🔋 **Spend Quality Time:** Parents should have regular family discussions with the children regarding digital devices and internet usage to understand their knowledge about online security issues. This will help the parents to assess and guide on media literacy and self-regulatory practices towards digital device usage.

   🔋 **Know About their Online Activity Pattern:** Help your child to make use of the technology and internet in the best way possible.

2. **Use of Digital Devices as Punishment/Reward:** As adoptive parents, discipline and routine are important to maintain a happy, stable home environment but it is not advisable to connect their good and bad behaviour with the use of digital devices.

🔋 **Keep Rewards and Punishments Out of Digital Devices:** Children tend to make mistakes in using media knowingly or unknowingly. Try to handle these issues with empathy and turn a mistake into a teachable moment. Do not use digital devices as a reward or punishment for your child's behaviour or blame them for getting into problems in cyberspace, this will create fear and they might start hiding things.

- Consider creating a rule/contract that is agreed mutually with consequences stated. However, remember the goal is not to punish but to set clear boundaries.

🔋 **Take Professional Help When Needed:** Parents should consider taking professional help, if the child is demonstrating strong signs of internet addiction.

3. **Learn and Explore Together:** Parents can help their child to develop the skills required to ensure safe learning environment by spending time together while exploring the digital world with enormous opportunities to learn.

🔋 **Discuss and Suggest** some good content for them to explore. Be supportive of online learning. Consider learning technology skills together.

🔋 **Stay Open-Minded:** Do not be too rigid towards your child's exploration of the internet and totally remove your child's phone/computer online access. This could isolate them from their peers and hinder their online learning. Rather teach them regulated usage with security awareness.

Build a Safe Environment at Home

A home is a place that gives a sense of security and safety. To ensure digitally safe and healthy environment at home, certain practices need to be followed.

1. **Digital Devices Under Parental Supervision:** Parents can help younger or older children to explore online, as well as help them to manage their accounts and compatible devices. Parents can monitor the child's online activity by using apps and setting screen time, etc.

🔋 **Use the Digital Device as Family Resource:** Computers and digital devices need to be treated as a common resource for the family. Placing computers in a common area of the house can help for easy monitoring of the child's online activity.

- Create a family media use agreement with all family members to encourage proper balance and use of technology.
- Establish limits, routines and guidelines.

🔋 **Set Screen Time:** Set reasonable screen time for any digital device including mobile, TV, computers, gaming consoles, etc.

🔋 **Apply Parental Controls:** Set parental controls on computers and other devices.

2. **Take Steps to Ensure Security:** Parents should orient their children about the cybercrimes and data breach which may happen while using the internet.

- **Secure your Wi-Fi:** Check devices connected with home Wi-Fi network and Secure your home Wi-Fi with a strong password.
- **Age Appropriate Use:** Ensure limited access to the websites. The access should depend on the child's age and level of maturity.
- **Turn off the GPS:** Using a simple GPS plug-in may lead to a potential stalker to drag uploaded photos from the internet and easily read the data connected to the pictures and track the child's location. Therefore, avoid publicly sharing your location in your digital devices.
- **Use Bookmarks/Starred Options:** Parents should make easy access to favorite sites and secured sites for their children.

Educating Your Child

In a world where children grow up along with digital devices which play an integral part in their life, it is important for parents to play an important part in teaching and helping them to learn healthy concepts of digital use. Parents may initially provide their support by constantly being with them and then retreat once their children have practised and gained confidence. Here are some ways in which parents can teach children about online safety:

1. **Stay One Step Ahead with Digital Skills:** To stay ahead and stay secure in the digital world, the child needs to think critically, observe, analyze and come up with **SMART** solutions. Parents need to be smarter to help their child navigate this world with the appropriate skills, behaviours and thinking, to become not only safe but also happy and resilient users of digital technologies.

Enable them to be '**SMART**' when they are online with the following aspects:

S	Stay Safe	- Never share personal information with anyone
M	Meetup	- Never meet with anyone you do not know
A	Accepting Files	- Never open or download the unknown files, pictures, mails
R	Reliable	- Verify the authenticity of the information received before proceeding to act
T	Tell Someone	- Inform trusted adult if you see/read something that makes you feel worried/ uncomfortable

Reference: *ThinkUKnow*

Discover the internet together with the child and discuss both positive and negative aspects to help them gain the knowledge and develop critical thinking to respond in the right way.

2. **Personal Information and Privacy:** Children tend to share a lot of personal information online. It is essential for children to understand the hazards of sharing personal information. Parents need to make them aware of many ways to protect personal information and privacy online. It is vital for both parents and children to learn about privacy settings. Awareness is the first step in online safety.

Importance of Personal Information: Make the child understand the importance of personal information and teach them to avoid sharing personally identifying information (e.g., real name, address, school, telephone number, photos, family member names) via the internet/any online medium.

- **Sharing Photos and Videos**: Discuss the potential problems associated with selfie culture and the possibility that shared images and videos could later be used in exploitative ways.

- **Importance of Passwords:** Educate children not to share passwords, even with their closest friend, and always close/sign out of their accounts before turning off computers especially in public places.
- **Importance of Financial Information:** Educate them to never share important credit/debit card details and let them know about the dangers and threats of free online offers or fraudulent email claiming huge rewards.
- **Use Privacy Settings Available:** Educate the child about privacy options on various digital devices and social media platforms. Review the privacy settings for posts, apps, and profiles. This way, it can be established which people get to see the child's profile and what they actually see; and to set the security features of browsers to "high".

3. **Pitfalls of Social Media and Safety Measures:** Social media connectivity presents positive opportunities and benefits as children use to chat with friends, network socially, share photos, make music videos, upload videos, play games, visit chat rooms, use file sharing sites, etc. At the same time, children may encounter the following online risks while using social media:

- **Online Chatting:** Keep the youngsters away from online chats and try to apply the old rule, "never talk to strangers". Also, discuss the dangers of meeting the person they befriend online without permission.
- **Online Grooming:** Educate children about online grooming and the hidden dangers from strangers trying to win a child's trust with wrong intentions.
- **Cyberbullying:** Discuss with children about cyberbullying and make them well aware that online harassment can cause grave emotional issues, therefore they should seek immediate help when required.

4. **Teach about the Darker Side of the Internet:** The internet is a great source of information for children, but they need to be aware of the hidden dangers of using it.

- 📋 **Need to Fact Check:** Teach the child about the huge amount of information available online and the possible ways to evaluate the authenticity of such information.

- 📋 **Avoid Unauthorised Websites**: Educate them to never visit unauthorised websites or sign up for every website. Many social networking sites (YouTube, Instagram, etc.) have age restrictions.

- 📋 **Malicious Links:** Inform children about the malicious links on video sharing sites like YouTube, Instagram, and alert them to avoid clicking on such links which offer exciting benefits.

- 📋 **Fake Profiles**: Educate the children about the celebrity chat groups/pages. They should be made aware that these celebrity social media accounts /pages may not be running by the celebrities or their fans, and they need to be cautious about it.

Enabling Security Features for Digital Safety

It is important that the parents are digitally aware and up-to-date to implement and enable some important security features and practices when they are online or are using the digital devices.

Basic Security Measures

- Ensure that all operating systems installed in your device are updated with the latest security updates as soon as they come out.

- Do not install any software without reading the license agreement and make sure your children ask for your permission before downloading or installing something on your devices.

- Do not execute online transactions on websites without 's' in their URLs https://. "S" in "https" stands for "secure".

- Do not share your financial details like credit/debit card/UPI on educational websites or gaming sites. Disable purchase options to avoid any unknown account charges.

Smart Ways for Digital Parenting

- Check with your Internet Service Provider for any parental controls, tools they may offer.

- Use filtering options for your child on browsers to avoid unnecessary websites with inappropriate content.

- Parents should ensure that they do not leave their devices unattended as children might explore or misuse the device.

- Discourage your child from downloading games and other media which could harm programs on systems by unauthorised users.

What are the major online security threats that children are likely to face?

Children are equally vulnerable to cybersecurity problems as much as adults. Some of the biggest threats faced by children are Scams, Identity piracy, free download dangers, cyberbullying, links to malicious sites, viruses, unwanted pornography, getting sexually solicited, etc.

How do I talk with my child about online security?

Talking to children is a two-way communication process that needs empathy and skill. In the current digital age, children are exposed to a lot of information which can be sometimes overwhelming for them. Parents need to be supportive and encourage open conversations within the family. Parents should put forth the possible online threats or dangers, and the necessary security measures to be adopted. They should explain to them the ethical practices to be followed and clearly lay out the best practices to be followed for the usage of internet and digital devices. The child should be encouraged to discuss their online issues and seek guidance.

How do we build a safe and healthy digital environment at home?

Parents need to mentor their children on following safe digital and internet practices when they are at home. They should make it a family practice and agree to not entertain digital devices during food time, study time, playtime and have limited screen time. Make the computer time to be a together activity rather than leaving the child alone with it. They should make children aware that using digital devices is a privilege and it should be responsibly taken up with care and caution. Also, the adults in the family need to enable the required security features on digital devices like ensuring the Wi-Fi is secured, that the operating system and the software used are up-to-date, installation of updated antivirus and malware protection software, etc.

Why do we always hear "Never share your passwords"?

Sharing passwords can lead to stealing of important information online and can end up in the hands of others. Sharing a password may lead your data and identity out of control. It is important that passwords are kept private, easy to remember and hard to guess.

How do we protect our mobile devices?

The best way is to use a strong password. We should be careful about what apps we use; there are security apps too for mobile devices that have a way of wiping your data if your phone is lost or stolen. Ensure that free or public Wi-Fi is protected and avoid turning on autofill, utilize VPN (Virtual Private Network).

The following statistical figures indicate that a good number of Indian children are engaging themselves online:

- **Internet and Mobile Association of India (IAMAI)** in its report titled 'India Internet 2019', stated that India had 451 million internet users, out of the 451 million monthly active users in India, 385 million are over 12 years of age and 66 million are in the age group of 5 to 11 years, who access internet on the devices of family members. It said that two-thirds of internet users in India are in the age group of 12-29 years.

- **Media use by Age, Children and Parents**: Media use and attitudes report 2019 by Ofcom, UK provides evidence on media use, attitudes and understanding among children and young people aged 5-15 years, and media access and use for young children aged 3-4 years. A snapshot of their study are shown in the following pages.

3-4 YEAR OLDS

- **24%** have their own tablet.

- **20%** use a smartphone to go online, and **49%** use a tablet to go online.

- **15%** of tablet owners are allowed to take it to bed with them.

- **11%** use a smart speaker in the home.

- **95%** watch TV on a TV set, while **36%** use a tablet. and **14%** use a mobile phone to watch TV.

- **98%** watch TV programmes or films (on any device), for **12 hours 42 mins** a week.

- **75%** watch live broadcast TV, and **65%** watch video-on-demand content*.

- **39%** play games, for **4 hours 42 mins** a week.

- **17%** play games online.

- **51%** watch YouTube, for **8 hours 6 mins** a week.

- **3%** watch YouTubers or vloggers.

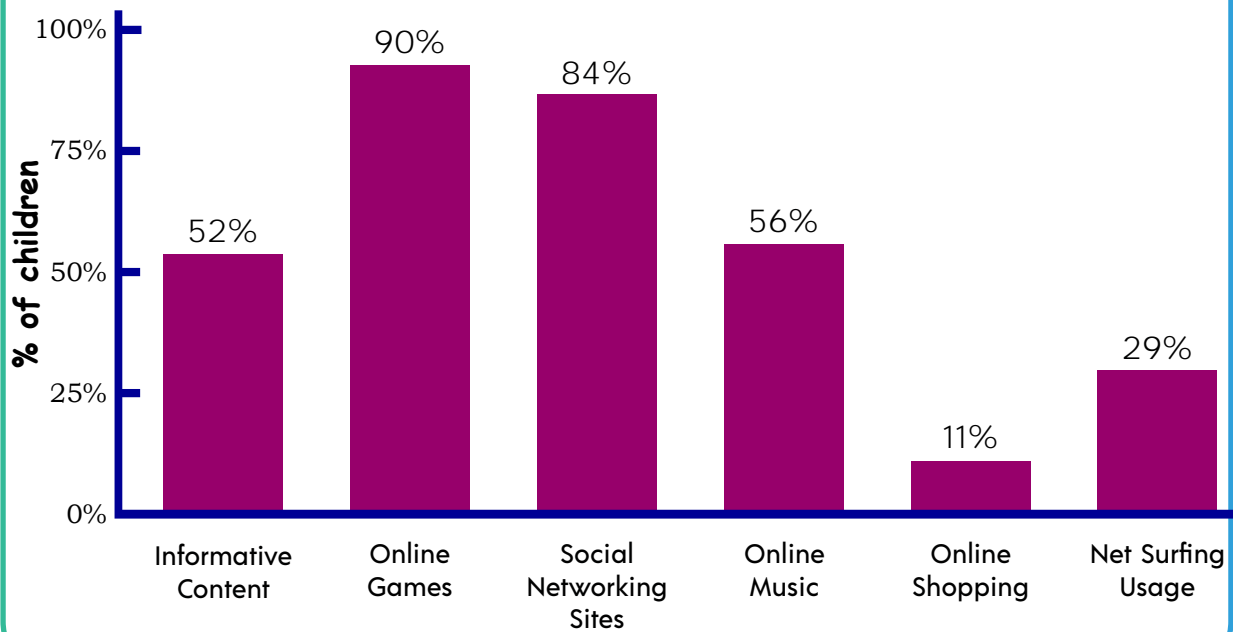- **1%** of online users have a social media profile.

5-7 YEAR OLDS

- **5%** have their own smartphone.

- **37%** have their own tablet.

- **27%** use a smartphone to go online, and **63%** use a tablet to go online.

- **14%** of tablet owners are allowed to take it to bed with them.

- **20%** use a smart speaker in the home.

- **96%** watch TV on a TV set, while **40%** use a tablet, **12%** use a mobile phone to watch TV.

- **98%** watch TV programmes or films (on any device), **11 hours 6 mins** a week.

- **73%** watch live broadcast TV, and **73%** watch video-on-demand content*.

- **62%** play games, for **6 hours 18mins** a week.

- **35%** play games online.

- **64%** watch YouTube, for **8 hours 36 mins** a week.

- **11%** watch YouTubers or vloggers.

- **4%** of online users have a social media profile.
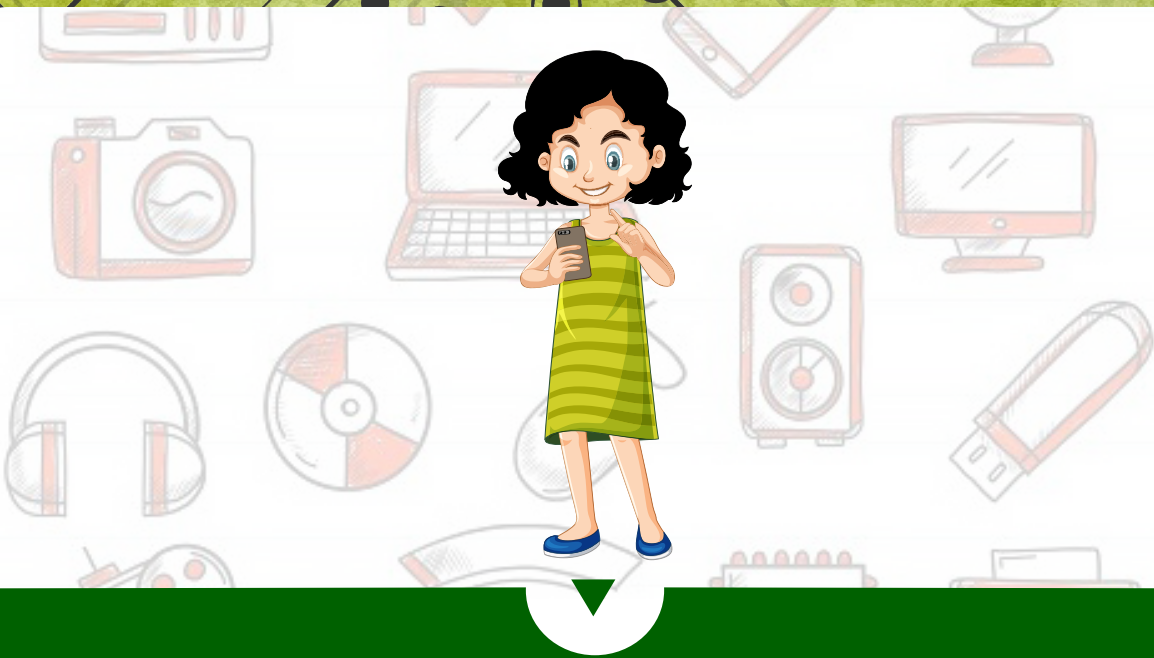
8-11 YEAR OLDS

🛡️ **37%** have their own smartphone.

🛡️ **49%** have their own tablet.

🛡️ **49%** use a smartphone to go online, and **72%** use a tablet to go online.

🛡️ **45%** who own a mobile phone are allowed to take it to bed with them, while **32%** of tablet owners are allowed to do this.

🛡️ **25%** use a smart speaker in the home.

🛡️ **92%** watch TV on a TV set, while **42%** use a tablet, and **22%** use a mobile phone to watch TV.

🛡️ **99%** watch TV programmes of films (on any device), for **10 hours 30 mins** a week.

🛡️ **74%** watch live broadcast TV, and **78%** watch video-on-demand content*.

🛡️ **79%** play games, for **9 hours 30 mins** a week.

🛡️ **66%** play games online.

🛡️ **74%** watch YouTube for **10 hours** a week.

🛡️ **27%** watch YouTubers or vloggers.

🛡️ **21%** of online users have a social media profile.

12-15 YEAR OLDS

🛡 **83%** have their own smartphone.

🛡 **59%** have their own tablet.

🛡 **81%** use a smartphone to go online, and **69%** use a tablet to go online

🛡 **74%** who own a mobile phone are allowed to take it to bed with them, while **61%** of tablet owners are allowed to do this.

🛡 **36%** use a smart speaker in the home.

🛡 **88%** watch TV on a TV set, while **46%** use a tablet, and **41%** use a mobile phone to watch TV.

🛡 **98%** watch TV programmes of films (on any device), for **11 hours 48 mins** a week.

🛡 **75%** watch live broadcast TV, and **88%** watch video-on-demand content*.

🛡 **81%** play games, for **11 hours 36 mins** a week.

🛡 **72%** play games online.

🛡 **89%** watch YouTube, for **11 hours** a week.

🛡 **41%** watch YouTubers or vloggers.
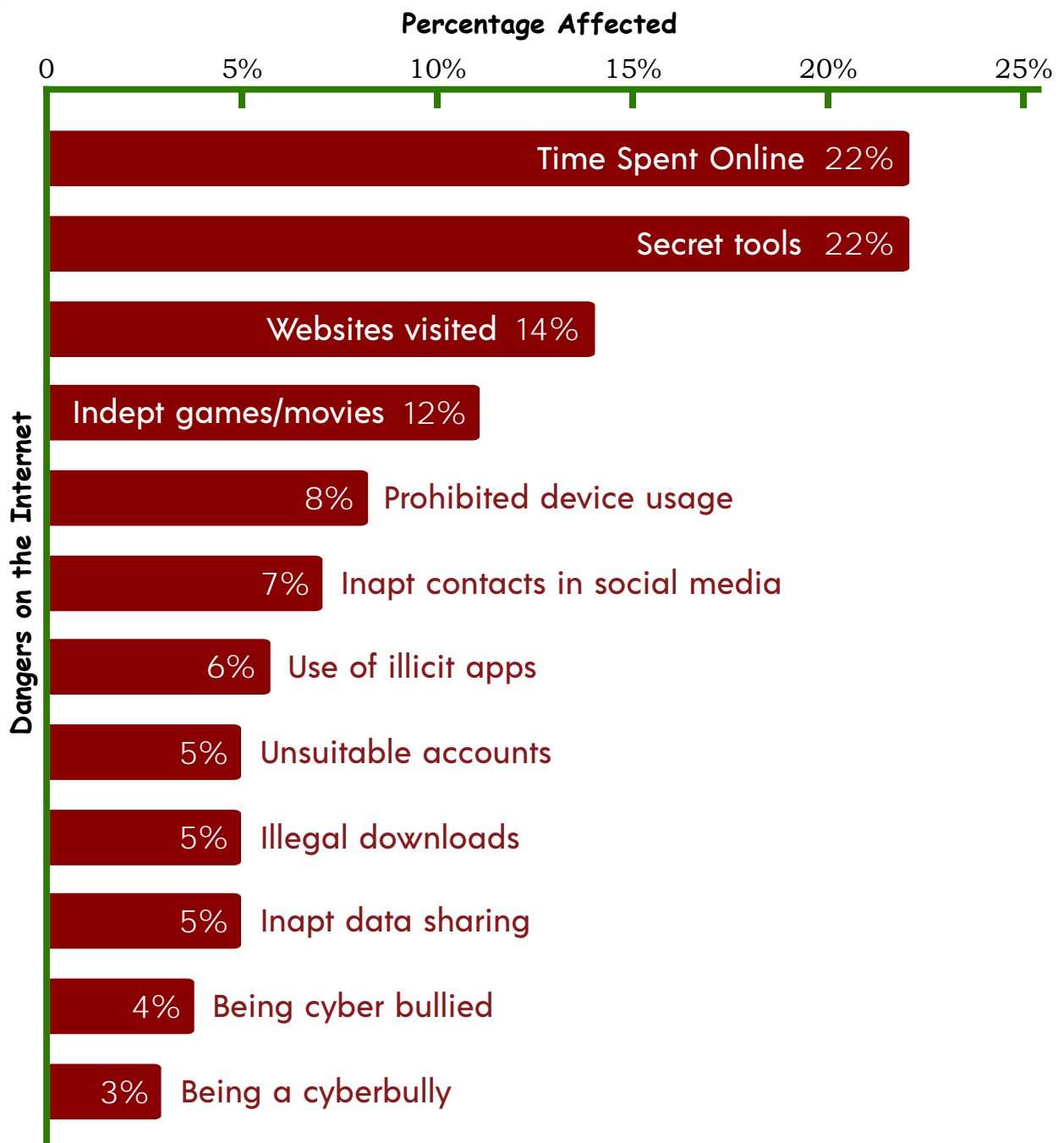
🛡 **71%** of online users have a social media profile.

🔋 According to the research paper *'A study of internet usage patterns among children of Indian urban families'*, submitted by Daman Deep Kaur Gulati, Assistant Professor B.S.S.S., Bhopal in 2018, 90% of the children use the internet for playing games and 84% for connecting on social networking sites.

% of children

Category	%
Informative Content	52%
Online Games	90%
Social Networking Sites	84%
Online Music	56%
Online Shopping	11%
Net Surfing Usage	29%

🔋 In addition, NDTV also reported (2017) that children in urban India within the age group of nine to seventeen years spend about 4 hours a day on the internet mostly through mobile phones. According to the survey by WebWise released by telecom operator Telenor, 134 million Indian children are estimated to come online. The mobile phone is the preferred access device for children and 62.4 per cent of them are spending upto 4 hours a day on the internet.

🔋 **The Telenor India WebWise** report (2016) indicates that children are extremely vulnerable to account hacking, receiving inappropriate messages, being bullied online, etc.

🔋 **Kaspersky Lab Research (2016)**: The dangers of excessive privacy were highlighted globally.

Percentage Affected

Dangers on the Internet

Category	Percentage
Time Spent Online	22%
Secret tools	22%
Websites visited	14%
Indept games/movies	12%
Prohibited device usage	8%
Inapt contacts in social media	7%
Use of illicit apps	6%
Unsuitable accounts	5%
Illegal downloads	5%
Inapt data sharing	5%
Being cyber bullied	4%
Being a cyberbully	3%

Inferences from Information Security Education and Awareness (ISEA) Workshops: Over the years ISEA has been interacting with children through awareness workshops and competitions across the country. During these interactions, it was found that a child spends an average screen time of 22 hours per week for various educational, entertainment, social interactions, creative work, etc. The drastic change across the world from March 2020 forced children and parents to be online for various educational and socio-economic necessities and it was found that the average screen time has increased to 48 hours per week.

All the above statistics and inferences indicate the dangers that the children are vulnerable to online risks and bring forward the aspects that need to be mainly addressed by parents like limiting screen time, need for best online practices to be followed, awareness about online threats/dangers, need for safety and security measures to be adopted.

Today technology has provided a huge platform with immense opportunities. Through the use of technology, we have access to information at our fingertips, it enables us to learn about new information and gain knowledge. It also presents us with a few challenges that we need to be aware of and prepared to overcome by adopting necessary security measures. We need to understand the advantages and disadvantages of the technology. We can effectively make use of these progressively useful aspects of technology, if we equip ourselves with the right knowledge, information, and practices for using them appropriately and safely.

In the current digital world, as parents of the digital age children, the right combination of digital knowledge, parenting skills, and security awareness is necessitated to be equipped. This helps us both nurture and mentor the children appropriately to evolve as digitally enabled netizens of this cyber age.

References

https://www.researchgate.net/publication/332107683_A_study_of_internet_usage_pattern_among_children_of_Urban_Families'

https://www.bloombergquint.com/technology/about-15-of-indias-internet-users-are-aged-5-11-years-says-iamai-report

https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627-million-in-2019-report/articleshow/68288868.cms

https://www.ndtv.com/india-news/indias-urban-children-spend-4-hours-on-mobile-internet-per-day-survey-1275223

https://www.infosecawareness.in/

For more details visit

· ·

www.ncert.nic.in

www.ciet.nic.in

www.ictcurriculum.gov.in

www.infosecawareness.in

www.cyberswachhtakendra.gov.in

विद्यया ऽ मृतमश्नुते

एन सी ई आर टी
NCERT

· ·

Central Institute of Educational Technology
National Council of Educational Research and Training
Sri Aurbindo Marg, New Delhi-110016

· ·