International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: *http://ijwos.com*
Vol.02 No.12.
OPEN ACCESS
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos02120324489

Cyber safety: Nurturing a Safe Online Ecosystem for Children in the Digital Realm

Mr. Utsav Singh[1], Dr. Monika Gautam[2]
[1] *B.El.Ed. (Batch 2023-2027), Amity Institute of Education, Amity University Uttar Pradesh, Lucknow.*
[2] *Assistant Professor, Amity Institute of Education, Amity University Uttar Pradesh, Lucknow.*

Article Info

Article History:

Published:15 Dec 2025

Publication Issue:
Volume 2, Issue 12
December-2025

Page Number:
354-359

Corresponding Author:
Mr. Utsav Singh

Abstract:

In modern times, children's familiarity with digital tools is reshaping their daily lives quicker than before. Digital technology has a great impact on the overall development of children. Constant use of devices like phones, apps, gaming platforms and social networks brings challenges like online bullying, exposure to predators, weak data safety and stolen identities. This may lead to anxiety, depression, isolation and poor performance in academics. The children may also show poor emotional regulation. Therefore, it is essential that efforts are made at different levels to keep children safe online. The present paper discusses the online dangers and how children can be kept safe while they are browsing the internet. It highlights the need for parental controls, strong passwords, privacy settings, screen time and knowledge of phishing and unsafe links.

Keywords: Online dangers, Cyber security, online platforms

1. Introduction

Technology is an essential part of modern society. Smartphones, tablets, social media platforms and virtual learning space have transformed the daily life of human beings. Access to information and execution of many different tasks has become easy and convenient due to technology. But it has also created problems related to violation of privacy and security of people. Children are increasingly using electronic devices from a young age. The internet provides them with information and entertainment but also presents serious threats and dangers to them. Cyber safety of children has now a matter of grave concern for parents, teachers, and policymakers.

Before the digital era, safety of children meant keeping them safe from physical harm, abuse and neglect. But in the present times, it includes protection from cyber threats. Digital safety includes protecting children from inappropriate content, cyberbullying, online predators and other types of online abuse. The Digital world does not have distinct boundaries. Risks lurk behind friendly interfaces and anonymous avatars. Children often cannot tell the difference between safe and unsafe interactions. When children go online, they are exposed to multiple dangers. Such threats can lead to direct and adverse consequences on their overall well-being and mental health. The different types of online dangers and threats are mentioned below:

Exposure to Inappropriate Content

Children may access content that is not appropriate for their age. They may watch violence, sexual or other unsuitable material. Sometimes obscene advertisements pop up on the website that children visit.

This may have profound impact on their psyche. They may not understand these in the correct manner. They may start having nightmares, anxiety and confusion about what adults do. The internet is inundated with wrong, inappropriate and misleading information that can adversely affect a child's understanding of the physical world. Such misleading information on health, social issues or global events can mould their beliefs and behaviors in a negative way.

Cyberbullying

When children are online their confidential information may be leaked and may be used for defamation or even fabricating a web identity through which cyberbullying can be done. Traditional bullying happens in specific physical locations while cyberbullying can occur from anywhere at any time which makes it ceaseless and widespread. Cyberbullying often leads to many psychological problems such as depression, anxiety, being socially isolated and in extreme cases may lead to suicide by the person. Facing online bullying often from anonymous people make a victim feel powerless. Victimization rates increased from 3.8% to 6.4% for females and from 1.9% to 5.6% for males over three years. This reflects a rapid increase in digital aggression in a national setting. Online harassment, trolling, exclusion, and impersonation were other prevalent modes of digital aggression. The psychological effects are also severe, with approximately 33% of females and 16.6% of males exhibiting symptoms of depression during young adulthood-a direct effect tied to such experiences..

Online predators

Predators use compliments, promise of gifts etc. to get the attention and trust of children and then exploit them. Children are naturally inquisitive and want love and from people. The predators compel children to share private information, participate in criminal activities and sexually exploit. It leads to anxiety, mental anguish, self-injury, or sometimes physical danger in cases where a predator meets the person in physical world.

Identity Theft and Privacy Violations

Children are not aware about how dangerous it can be to share personal data online. Cybercriminals take advantage of this and steal personal data of children when these children use different online platforms. This information can be used to create fake identity, fake accounts, financial exploitation, or other crimes that may have dangerous repercussions for the children.

Phishing: Cyber criminals use phishing to trap victims online and steal their private data through counterfeit emails, texts, or websites.

2. Impact of Online Dangers on Children

Exposure to online threats has far reaching consequences. It has a deep impact on the child's psycho-emotional development and behaviour. Below are the impact of Online dangers on young minds:

Psychological and Emotional Effects

Children who face bullying or threats online often face mental and emotional problems. It leads to problems of depression, anxiety, and post-traumatic stress disorder (PTSD. Victims of cyberbullying often withdraw from the world around.

Children who watch violent and disturbing content online often struggle and face difficulties in regulation of their emotions. They may have anger issues and experience fearful nightmares, A child's

self-concept may suffer when he or she constantly watches unrealistic portrayals of relationships, body image, and behavior.

Behavioral Consequences

Youngsters who are bullied online often become withdrawn, reclusive or show sudden mood swings. They may withdraw from friends, lose enthusiasm for activities, exhibit signs and symptoms of panic including crying, mood tantrums or even lack of concentration. They may also start copying the negative behaviour that they see online. Internet anonymity and the absence of immediate repercussions can make young people start cyberbullying, sexting, or talking with strangers. Such behavior endangers them and also starts off a vicious cycle of harm and transform the internet into a hostile place. Due to Cyberbullying young people may face a lot of difficulty in trusting people and may face severe problems in interpersonal relationships and communication.

Educational consequences

Children who face problems and threats on the online platforms often show poor performance in academics. Their attention, motivation, and general cognitive ability are affected negatively.

3. Cyber Security for Protection of Children in the Digital Age

The variety of threats that are widespread in the digital world have serious influence on the overall well-being of children. Steps and measures need to be taken timely to ensure that children are safe and secured from all types of online dangers.
Some of these measures are mentioned below:

Parental Controls: Software applications are available which help parents to limit the use of internet by children. This helps in monitoring the sites visited, setting time limits on use of device and screening out unsuitable material. Supervision and vigilance by parents plays a very significant role in ensuring the safety of children especially when they are online.

Use of Strong Passwords: Children should be informed and guided about how to create and use strong passwords as well as and turning on two-factor authentication so that they are safe online. The passwords should include numbers, letters, and symbols. Children should be taught to use passwords that have at least 12-16 characters, uppercase, lowercase, numeric and special characters. They should avoid the use of easily guessable information like birthdays. They should regularly change their passwords and ensure that the new password is not like the previous ones. They should not share passwords with anyone. A unique and strong password provides a strong line of defense. Having 2 Factor Aunthentication enabled on all accounts adds an extra level of protection. Confirmation through the use of a second method like a code sent to phone or Email add protection to account. Password managers help to securely store and generate strong passwords. This helps to eliminate the chance of reuse of password across devices.

Education on Privacy Settings: Parents should educate children about how to regulate privacy settings on social media and other sites to ensure that their personal information cannot be accessed by others.

Secure Wi-Fi connections: It should be clearly informed to children that they should not use public networks as these may be easily hacked. Internet Networks at home should always be password protected and regularly updated with security updates.

Regular software updates: The children should be guided to regularly update their devices and keep software updated. This will help in lowering damage by the new security risks.

Digital Literacy and Cyber Hygiene

Digital literacy is very important for online safety of children. They should be taught about how to identify risks like phishing emails, suspicious links or downloads. They need to be told about how to evaluate online content. Parents should make the children aware that they should check facts that are presented online, recognise biased or fake news and should always remember that everything they do online leaves a trail. This will help children in the wise navigation of websites and stay safe online.

4. Use of Technology in Enhancing Cyber Security

Technology can be very helpful in protecting children from online abuse. Tools like AI-driven content filters, anti-bullying software, and real-time monitoring apps can help keep them safe online. There are Machine learning algorithms that can monitor and prevent the child from viewing inappropriate content, notice strange behavior and notify adults about possible dangers. While software can help shield children from certain threats, it is not a substitute for the critical thinking skills and digital literacy that children need to use to stay safe online. They should be educated to see whether links are real. They should look for 'HTTPS' in a website's URL to avoid counterfeit pages.

Facing phishing: Children should be eduacted about what is phishing and how to fight it. Users need to be on the lookout for phishing emails that ask them to share personal information, or intimidate them into providing information or doing something immediately. They should be told about dangers of sharing personal information online and also that they should always tell their parents if they get a strange message.

Reducing Screen Time : Excessive screen time adversely affects children's physical and mental health, leading to issues including sleep loss, eye discomfort, and reduced social engagement.

Promoting Positive Online Interaction : Children should be encouraged to follow digital citizenship. They should interact cautiously with others on the online platform.

Legal Frameworks and Policies on Child Cyber Safety

The IT Act 2000 is one of the first legislation in India dealing with the legal aspects of cybercrimes, cyber frauds and misuse of electronic data. It has also been amended to provide harsher penalties for such crimes and enables the state's investigating authorities to take action and discipline/rectify such cyber-criminal behaviours. The Protection of Children from Sexual Offences (POCSO) Act, 2012 also aims to provide complete protection to the child from various forms of sexual abuse and exploitation, including digital crimes as well, and thus, is a useful complement to the IT Act.

The Digital Personal Data Protection Act, 2023 is aimed at providing a legal framework for data processing and speedy responsible data handling. Numerous cyber safety and digital awareness campaigns led by MeitY are also going on. India's National Cyber Security Policy aims to create a secure digital ecosystem especially for children and protect them from negative influences of cyberspace. The primary aim of all these laws and policies is to assist in protecting children from the multitude and ever-increasing detrimental aspects of the digital world.

Install software updates and security measures regularly : Regularly updating devices helps in safeguarding against cyber attacks. By allowing automatic updates, devices can be kept secure. Some

programs like, installing trustworthy antivirus software and scanning computer on a regular basis can help identify and eliminate malicious programs before any serious damage occurs. Use of firewalls provides defense by preventing unauthorized access to devices and networks. Children should always ensure that they log out from shared devices and should avoid using Wi-Fi of public places. These practices will help in the reduction of cyberattacks and help children stay safe when they are donline.

No sharing of Personal Information: Children should be strictly told never to share their personal information on online platforms and with strangers.

Think Before Clicking: Children should always check online links or attachments, especially those from unknown senders, before clicking/opening them. If an email claiming that a person has won a free gift or prize, then they should not respond to the mail nor click any link. Links in unexpected emails or messages should not be opened.

Report and Block Suspicious Behavior: When children face harassment, bullying or abuse digitally they must immediately inform their parents. If any website or person seems doubtful, then they should be immediately blocked.

Set Boundaries and Time Limits: Children who are active online for many hours are at greater risk of becoming victims of different types of cyberbullying and threats. Therefore, parents should take strict steps to reduce screen time of children.

No interaction with Strangers online: Children should stay alert online and must never respond to strangers who contact them online.

Use of Safe Search Engines and Platforms: Children must use safe search engines and access online platforms cautiously.

Role of Teachers and Parents

Teachers and parents have a very significant and crucial role in ensuring the safety of children when the latter are safe online. Their role is listed below:

Role of Parents

Parents play a very important role in the development of digital habits in children. They have to practice responsible online use and share the best practices of how to use technology in a mature and ethically sound way. Parents must communicate with children about the dangers and reality of internet use. They should guide them about responsible online surfing and what are the best practices regarding use of technology. Parents should converse with children about cyberbullying, privacy, and digital etiquette teaches so that children are able to make wise decisions in the use of technology and internet. Parents should behave wisely and create an environment at home in which children share their experiences and feelings freely.

Role of Teachers and Schools

Teachers should guide children and ensure that they follow digital citizenship. They should help children in staying safe online as well as make them aware about where to report if they face cyberbullying. The must be vigilant and observe modifications in behaviour that indicate that a student is struggling with cyberbullying or other challenges online. Schools should regularly organize events

like workshops and lectures in which cyber experts interact with children and guide them about staying safe online. Schools and parents must work together to ensure that children stay safe from online abuse.

5. Conclusion

Today it is very easy to quickly access information online from all parts of the world. But this convenience comes with many threats and safety concerns. Cyber safety is the responsibility of parents, teachers, technology developers, and children themselves. Children should be encouraged to browse internet responsibly and use robust cyber security measures so that they always stay safe online.

References

1. Livingstone, S., & Haddon, L. (2020). Theoretical frameworks for children's internet use. *Journal of Media Literacy Education, 12*(1), 1-18.
2. Hinduja, S., & Patchin, J. W. (2019). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying.* Sage Publications.
3. Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2019). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49*(4), 376-385.
4. Olumide, A. O., Adams, P., & Amodu, O. K. (2020). Online child grooming and children's risky online behaviors. *Child Abuse & Neglect, 101*, 104-115.
5. Chassiakos, Y. R., Radesky, J., Christakis, D., Moreno, M. A., & Cross, C. (2018). Children and adolescents and digital media.
6. Silent Screams: A Narrative Review of Cyberbullying Among Indian Adolescents https://pmc.ncbi.nlm.nih.gov