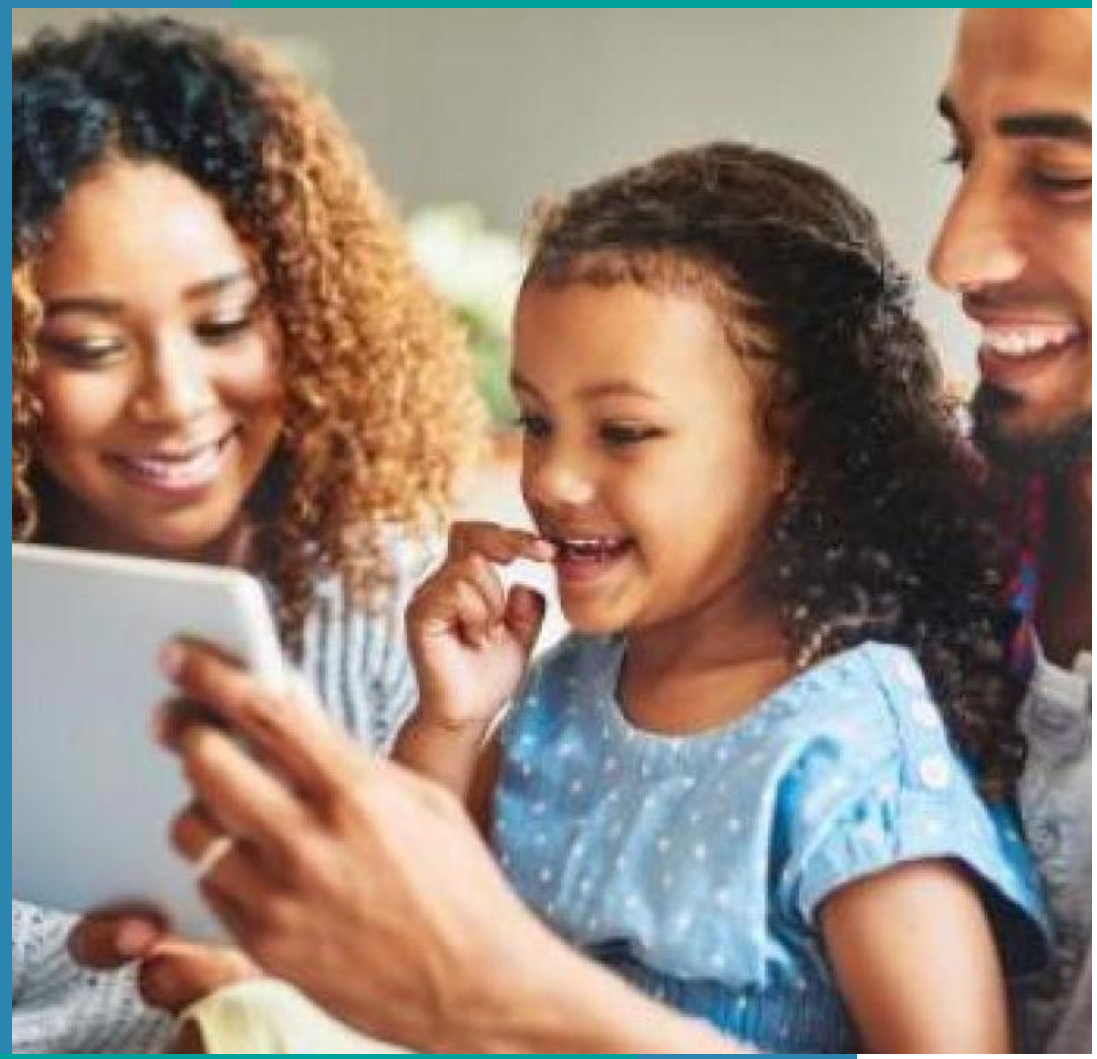
Safeguarding Children Online

Powered by: ISY-Internet Safety for Youth

Introduction: In today's digital age, ensuring the safety of children online has become more critical than ever. While the internet offers numerous opportunities for learning and social interaction, it also presents risks such as cyberbullying, inappropriate content, and privacy breaches. Today’s children are learning about the world through the internet, but this is not the same as learning through books, school teachings, or the knowledge of their parents. Safeguarding requires a collaborative approach involving parents, educators, and adults, with a focus on vigilance, education, and proactive measures.



What is Cyber Security?

- Cybersecurity refers to the practice of protecting systems, networks, and data from unauthorized access, attacks, or damage.
- It involves the use of technologies, processes, and controls to safeguard digital information and ensure the safety and privacy of users.
- Cybersecurity is essential to protect family members—especially children—from online threats such as cyberbullying, hacking, and exposure to inappropriate content.

why it's important for kids to understand cybersecurity.

It's important for kids to understand cybersecurity because they are increasingly exposed to the internet for learning, entertainment, and socializing. Without proper knowledge, they may fall victim to online risks such as cyberbullying, exposure to inappropriate content, and interaction with strangers. Teaching kids about cybersecurity equips them with the skills to protect their personal information, recognize threats, and navigate the internet safely. This early understanding fosters responsible online behavior, ensuring they are better prepared to handle the digital world securely.

The Growing Internet Usage Among Children

After the pandemic, both children and adults have become heavily reliant on online platforms. During the lockdown, children spent much of their time using devices for school, entertainment, and social interaction. This increased exposure makes it crucial for kids to understand cybersecurity. Without proper guidance, they risk encountering threats like cyberbullying, inappropriate content, and online predators. Teaching children cybersecurity practices helps them protect personal information, recognize dangers, and safely navigate the digital world, promoting responsible online behavior from an early age.

Online Threats for Kids

Common Online Threads

Inappropriate Content	Cyberbullying	Online Gambling	Pornography and Sexual Content
Material not suitable for children, including explicit, violent, or harmful content. This can negatively affect a child's emotional and mental development and is often found on websites, social media, and online games.	Cyberbullying involves using digital platforms such as social media, messaging apps, and online games to harass, threaten, or embarrass others. It includes actions like spreading rumors, sending abusive messages, or sharing private information. Unlike traditional bullying, cyberbullying can happen anytime and reach a wide audience quickly, causing emotional and psychological harm, such as anxiety or depression. The anonymity of the internet often makes it harder to stop and identify the bully.	Exposure to gambling websites or games with features like loot boxes or betting systems that imitate real gambling. These can encourage risky behavior and lead to unhealthy habits, especially for impressionable children.	Exposure to explicit material, such as pornography, can negatively impact a child's emotional and psychological development. It may lead to confusion, anxiety, or distorted views about relationships and sexuality

Strangers and Online Predators

Danger of Strangers

Strangers pretending to be someone else online can deceive children into sharing personal information or engaging in risky behavior. They may use manipulative tactics to build trust and exploit the child. Consequences can include identity theft, exploitation, or harmful encounters, which may lead to emotional distress, anxiety, and a sense of betrayal.

Fake Social Media Accounts

Fake Social Media Accounts can deceive children by impersonating trusted figures or creating false identities. This can lead to privacy violations, as personal information may be collected and misused. Children might experience emotional distress from the betrayal or manipulation, and there is a risk of exploitation or scams that could result in further harm or financial loss.

Online Grooming

Online Grooming involves predators building trust with children through online interactions to exploit or abuse them. This manipulation can lead to emotional and psychological harm, including anxiety, depression, and a distorted view of relationships. Victims may also face direct exploitation or abuse, which can have long-term effects on their safety and well-being.

Device Security

Weak Passwords

Weak Passwords are easily guessable combinations that can compromise account security. If children use simple or common passwords, it increases the risk of unauthorized access to their online accounts. This can lead to data breaches, identity theft, and unauthorized activities on their accounts, potentially resulting in loss of personal information or exposure to online threats.

Unsecure Wi-Fi

Open Wi-Fi networks that lack proper security measures. Connecting to such networks can expose devices to hacking and unauthorized access, leading to potential data theft, malware infections, and privacy breaches. Children using unsecure Wi-Fi may have their personal information compromised, which can result in identity theft or exposure to harmful content.

Excessive Screen Time

Too many hours on devices, which can lead to digital addiction and a range of health issues. Prolonged use can contribute to eye strain, poor posture, and sleep disturbances. Additionally, excessive screen time may impact social interactions and academic performance, and increase exposure to inappropriate content or online risks.

Malicious Software

Types of Malware

Malware include viruses, spyware, and other malicious software that target devices to cause harm. Viruses can corrupt or delete files, spyware can secretly gather personal information, and other malware can disrupt system operations. The consequences include data loss, privacy breaches, and potential financial losses if sensitive information is stolen or systems are compromised.

Phishing Emails

Phishing Emails are deceptive messages that appear to be from trusted sources, trying to trick kids into downloading harmful files or sharing personal information. If a child falls for a phishing scam, it can lead to their personal data being stolen, which might result in identity theft or unauthorized access to accounts. Additionally, it can expose their device to malware, causing further issues like slowing down their computer or losing important files.

Ransomware

For kids, encountering ransomware can result in the loss of access to important files, such as schoolwork or personal photos. It can also lead to financial issues if a ransom is paid, and it may require significant time and effort to clean the device and recover lost data.

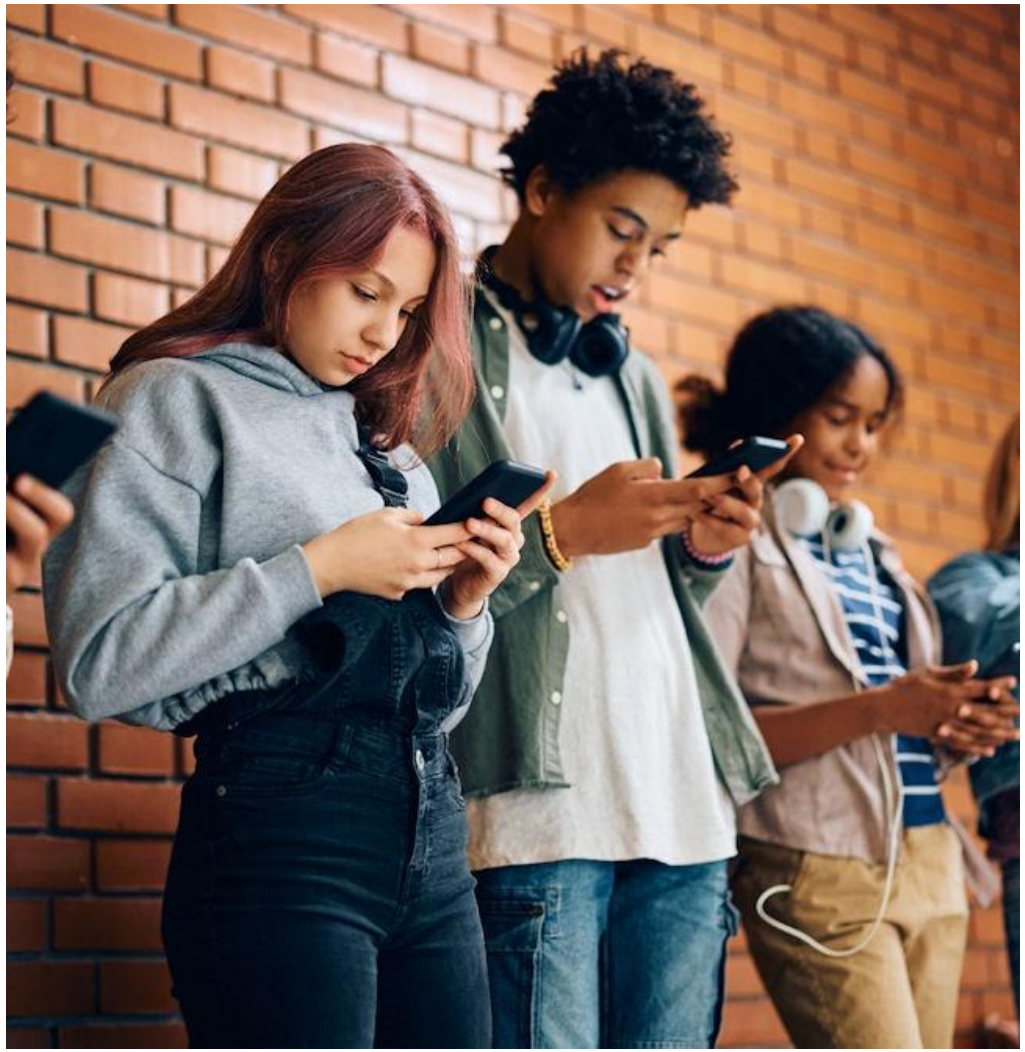
Social Media Dependency

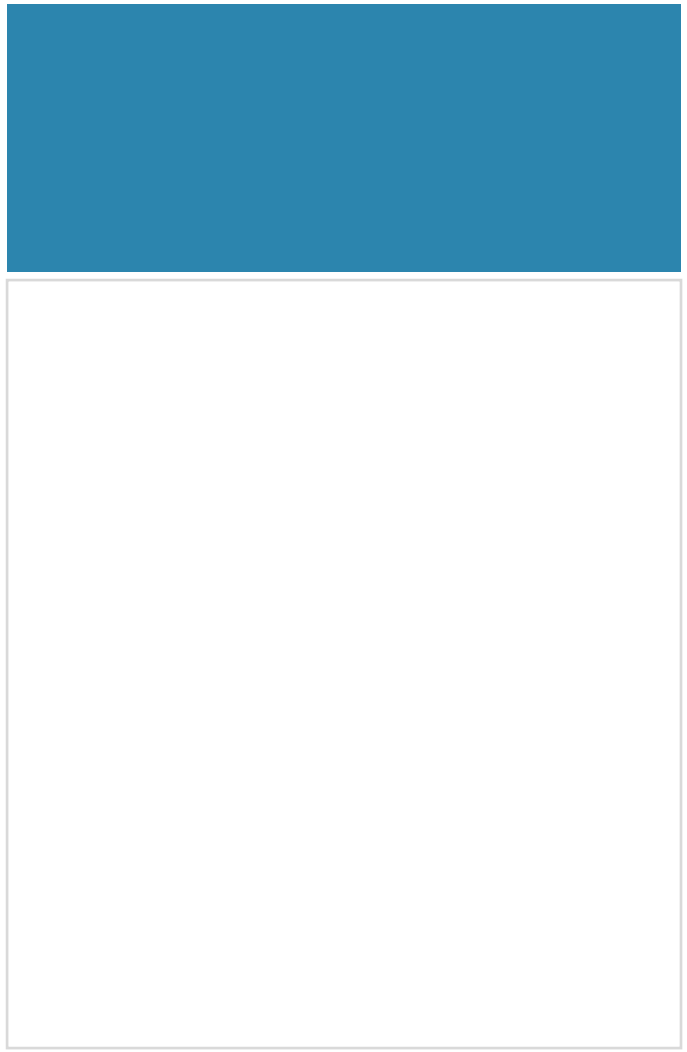
Sharing Personal Information

It involves disclosing details like addresses, phone numbers, or personal interests online. For kids, this can lead to privacy issues, including unwanted contact from strangers or potential identity theft. It may also make them vulnerable to scams or online predators, and can lead to emotional distress if their information is misused.

Oversharing on Social Media

posting excessive personal information, which can invite risks like privacy breaches and unwanted attention. For kids, this might lead to identity theft, cyberbullying, or exploitation by strangers. Excessive sharing can also impact their reputation and safety, making them targets for online scams or predatory behavior.





The Role of Parents, Educators, and Community in Cybersecurity

What can parents do to keep their children safe on the internet

- Monitor Online Friends
  - Encourage cautious trust.
  - Keep track of their contacts.
- Manage Device Access
  - Place screens in common areas.
  - Restrict private use of smartphones/computers.
- Foster Open Communication
  - Discuss online activities openly.
  - Be friendly to encourage sharing.
- Set Online Safety Rules
  - **Beware of Strangers:** Don’t meet unknown individuals; protect personal info.
  - **Keep Information Private:** Avoid sharing phone numbers, addresses, or locations.
  - **Password Safety:** Use strong passwords, don’t share them, and always log out.

The Role of Schools and Educators in Cybersecurity

- Implementing Digital Literacy in Curricula:
  —Schools should include lessons on safe internet use, recognizing cyber threats, and digital citizenship.
- Cyberbullying Prevention:
  —Teachers should recognize signs of cyberbullying and implement clear reporting procedures.
- Classroom Monitoring Tools:
  —Use educational tools to monitor internet usage in classrooms to ensure safety.

Social Community's Role in Cybersecurity for Children

- Support Initiatives:
  - Partner with schools and NGOs to implement and promote cybersecurity programs.
- Facilitate Support Networks:
  - Create spaces for parents and guardians to exchange advice and experiences.

The Role of ISY- Internet Safety for Youth

Educational Programs

ISY provides comprehensive educational programs aimed at enhancing child cybersecurity. These programs include interactive workshops and online resources designed for both children and parents. They cover a wide range of topics, from understanding various online risks such as cyberbullying, phishing, and privacy breaches, to teaching safe practices for using digital platforms. The programs also equip participants with skills to identify and handle online threats effectively, ensuring that both children and their guardians are well-prepared to navigate the digital world securely.

Parental Support

ISY offers resources to help parents understand digital platforms, set appropriate security settings, and recognize signs of online threats. This includes, ISY supports parents in having meaningful conversations with their children about safe online practices and addressing any cybersecurity concerns that may arise.

Awareness Campaigns

ISY conducts awareness campaigns aimed at educating youth about the importance of online safety and privacy. These campaigns focus on raising awareness about various online risks, including cyberbullying, privacy breaches, and the consequences of excessive social media use. Through engaging and informative content, ISY helps young people understand how to protect themselves online, make informed decisions, and recognize the signs of potential threats. The goal is to empower youth with the knowledge and tools needed to navigate the digital world safely and responsibly.

Support Services

ISY offers dedicated support services to assist with concerns related to cyberbullying and online threats. This includes providing personalized advice and solutions for addressing incidents of cyberbullying, helping families manage online safety issues, and offering guidance on dealing with various digital threats. By providing direct support, ISY helps ensure that children and their parents have access to the resources and assistance they need to handle online challenges effectively.

Trustee of ISY- Internet Safety for youth, Bangladesh

EHSAN HAQUE

Ehsan Haque is based in Switzerland; he is an accomplished senior level manager with an extensive background in Banking, with a track record in asset management, securities trading, FX, fund raising, communications and marketing. Ehsan's career has contributed on furthering the missions, initiatives and goals of organizations by being extremely focused in maintaining long-term objectives of the firms and their clients. Able to adapt to changing market conditions, especially in the financial sector, he helped teams analyze and think through the change process to acclimatize quickly to the sector's needs. Ehsan has worked as senior director positions in global financial institutions, including HSBC, RBC, Bear Sterns and Merrill Lynch, in London and Switzerland. He has studied computer science at the University of Massachusetts before completing his studies in Business and Human Resources Management at Palm Beach Atlantic University (US).

Conclusion: Safeguarding children online requires a united effort from parents, educators, and the community. By understanding the potential risks and implementing effective strategies, we can create a safer digital environment for our youth. Ongoing education, open communication, and proactive measures are essential in protecting children from online threats. Together, we can empower them to navigate the internet safely and responsibly, ensuring their well-being in an increasingly connected world.

Thank You!