CyberPeace
Foundation

Digital Parenting

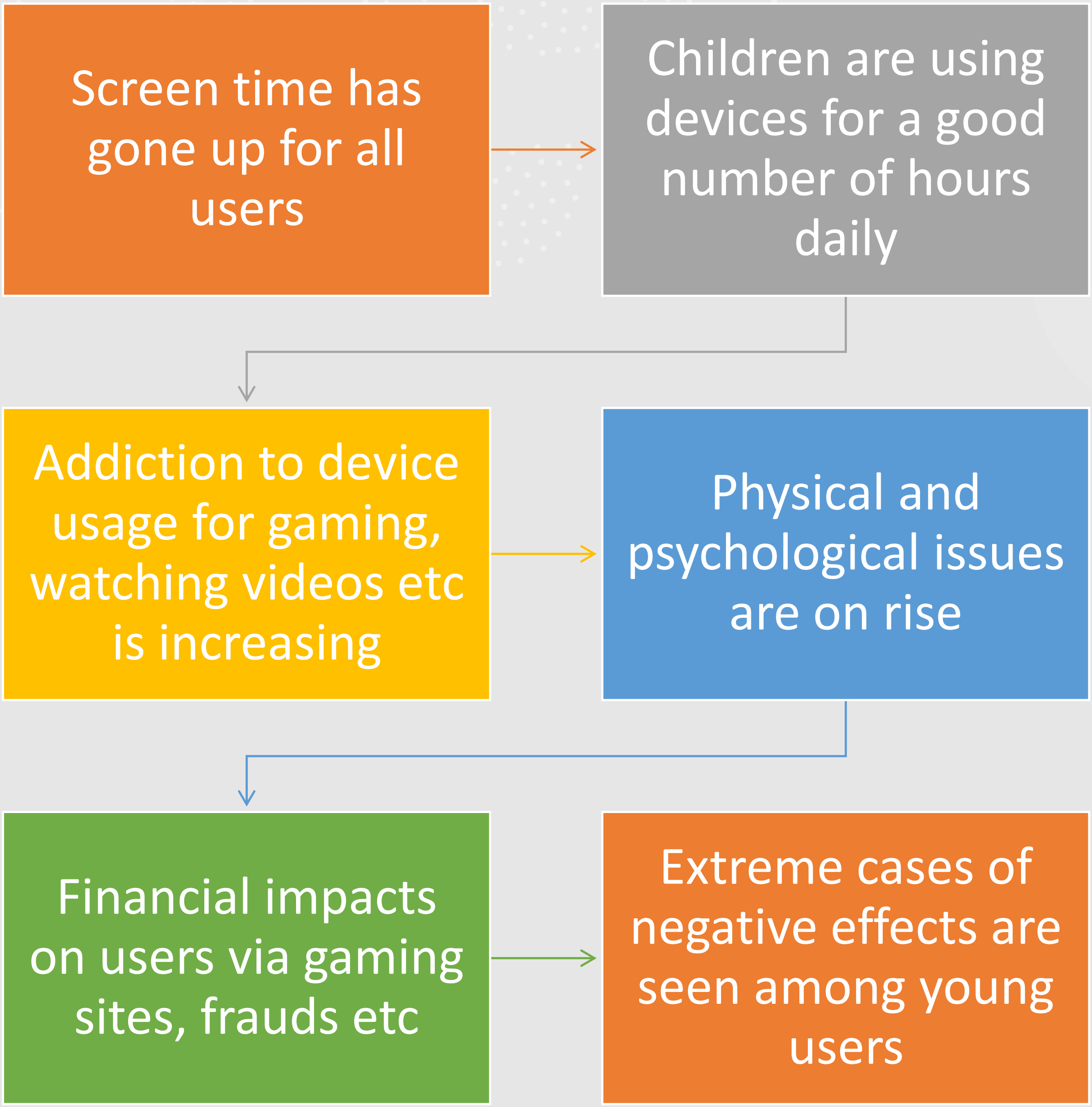
CyberPeace Foundation

Tech Penetration

- Usage of technology and devices have gone up multifold.
- Last mile reach has gone up
- Almost everyone in the family uses a device for day-to-day tasks or social connect
- Usage is quite high in younger generation
- Educational activities uses the technology dominantly
- Businesses are using technology

CyberPeace Foundation

Problem Statement



Screen time has gone up for all users

Children are using devices for a good number of hours daily

Addiction to device usage for gaming, watching videos etc is increasing

Physical and psychological issues are on rise

Financial impacts on users via gaming sites, frauds etc

Extreme cases of negative effects are seen among young users

How should we intervene

CyberPeace Foundation

- Partnering with children
  - Learn together new applications usage, their safety and privacy features
  - Discuss the new learnings on frequent basis
  - Use child friendly games which can be played online
- Increasing the digital literacy level among parents
  - Make effort to learn the new things in the digital world
  - Take time to go through the safety and privacy features/Help Centres of social media platforms
  - Use and explain the usage of strong passwords

CyberPeace Foundation

Intervention…

- Digital Literacy
  - Make effort to learn the new things in the digital world
  - Take time to go through the safety and privacy features/Help Centers of social media platforms
  - Use and explain the usage of
    - Strong passwords
    - Two factor Authentication
    - Private profiles
    - Audience control on social platforms
    - Safe downloads

Intervention…

CyberPeace Foundation

- Be vigilant of the kid’s online activities
  - Check the device at least once daily and browse through
  - Keep a check on the interactions that are taking place on various platforms
- Help them Understand the pros and cons of Digital world
  - Explain Digital Footprint to the kids
  - Help them learn about Empathy and responsible online behavior
  - Explain the risks of being negligent or complacent online

Intervention…

CyberPeace Foundation

- Spare time to discuss daily usage.
  - Discuss with the child the usage of device and platforms on frequent basis
  - Keep an eye on the screen time and put a routine around the same
  - Explain the benefits of judicious usage and encourage them to learn new things
- Use Parental controls
  - Available on most of the platforms
  - You can block unwanted content from being displayed to the child
  - Helps in keeping a check on the usage of the device by the child

CyberPeace
Foundation

Reporting

Local Police

Helplines

Report on Platforms

Decide what might work best in your situation!

What can you report to platforms?

- Report a user/account to the platform for objectionable behavior or any behaviour that you have a problem with
- Report specific posts/comments/other activity to the platform to review
- Unfollow/Block a user to stop them from contacting you
- Reporting may also help delete objectionable content and accounts

CyberPeace Foundation

Key Tips

Passwords

- Never use a guessable and common password for any account

- Have different passwords for all your accounts and manage them using a password manager

- Use additional layers of authentication called Two Factor Authentication (Preferably App based) for your internet banking, social media, email accounts etc.

- Never share your password with anyone, no matter who. A password is sensitive and personal.

CyberPeace Foundation

Key Tips

Emails

- Never open mails or click on attachments from unknown senders
- Always verify the Email ID of a mail sender, don’t trust a display name
- Don’t share highly sensitive and personal information over Email
- Whatever your Email service provider, review security, safety and privacy settings from time to time
- Always keep a working alternate Email ID, phone number and other methods of account recovery in case you lose access to your account.
- Try to set up different email accounts for work and social usage
- Avoid accessing Emails while on public or unprotected WiFi

Key Tips

Social Media

- Be cautious of who you befriend on Social Media, know their real identities
- Click links carefully, don't open a catchy headline if it looks fishy
- Be careful about the information you share on Social Media including images, videos, contact information, location information etc. and control the audience for all information you share
- Be wary of the privacy, security and conduct policies of all social media services that you use and be sure to implement them in practice
- Always be aware of what you are sharing on social media, mere sharing of a post can subject you to unnecessary trouble
- Review your security and privacy settings often

Key Tips

General Safety

- Try to never log into any accounts on unknown or untrusted systems. But if you do, log out after you're done.

- For all websites you visit, ensure that the URL is correct, the organization or individual is legitimate, language and content is not fishy and before entering your credentials, the URL reads https://.

- Download applications and other media from trusted and verified sources only. An unidentified source can infect your device and steal your data

- There's no free lunch. Don't reach out for trying to download movies, music and applications that are paid otherwise and you want them free. Such websites may land you into traps.

Thank You!

CyberPeace Foundation

Helpline No.: +91 957 00000 66

Website: www.cyberpeace.org