

सुरक्षित इन्टरनेट, सधैका लागि , सबैका लागि

Safer Internet Day Celebration

2025

Program Completion Report



Organizers



In Collaboration with:



Joining Forces are:



SUMMARY

Webinar on Child Online Safety: A national-level webinar was organized on the occasion of Safer Internet Day 2025. The Nepal Telecommunications Authority jointly organized the program with the Ministry of Communication and Information Technology, the Ministry of Women, Children and Senior Citizens, the National Child Rights Council, the Net4Good Alliance, Creation Society Nepal, and Joining Forces Nepal. The event invited experts from various children and online protection-related organizations as representatives from the Nepal Telecommunications Authority (Bijay Kumar Roy), National Cyber Security Center (Rajkumar Maharjan), Cyber Bureau of Nepal Police (Umesh Prasad Sah), and Office of the Attorney General (Bina Dahal) to discuss the importance of safeguarding children in the digital age. A renowned celebrity and media personality, Mr. Raja Rajendra Pokhrel, facilitated the whole webinar, including the panel discussion. During the webinar, panelists shared the major policies, practices, and gaps in child online protection and the legal aspects of online safety. The panelists also shared some cases and evidences on child online protection. Throughout the panel discussion, some queries were also raised by the participants and addressed by the respective panelists. Finally, the respective shareholders shared some key messages including National Child rights Council (Ram Bahadur Chand) and the session was wrapped with closing remarks from Ministry of Women, Children and Senior Citizens (Joint Secretary Mr. Chakra Bahadur Budha).

National Workshop on the Role of Government and Service Providers for Safer Internet: Nepal Telecommunications Authority (NTA) organized this workshop in collaboration with key ministries, regulators, and civil society organizations, in presence of 144 participants in order to address Nepal's evolving cyber challenges. Representatives from Internet Service Providers Association of Nepal (ISPAN), Ncell Axiata Limited and Nepal Doorsanchar Company Limited (Nepal Telecom) highlighted efforts to combat vulnerabilities like data leaks and tracking, while representative from Nepal Rastra Bank outlined practices and plans for digital financial regulations. Representative from Cyber Bureau reported alarming cybercrime trends, with 20,000+ cases targeting women and children, underscoring gaps in resources, cross-border coordination, and forensic capabilities. A moderated panel stressed collaborative governance, public-private partnerships, and inclusive policymaking to address implementation gaps, while guests emphasized child protection, grassroots awareness, and ethical AI use.

Key outcomes included strengthened stakeholder networks, commitments to digital literacy campaigns, and prioritization of legal reforms. Challenges such as underreporting, resource constraints, and balancing security with accessibility were met with recommendations for enhanced technical capacity, unified frameworks, and nationwide cyber hygiene initiatives, collectively advancing Nepal's safer digital ecosystem.

सारांश

अनलाइन बाल सुरक्षा सम्बन्धी वेबिनार: सुरक्षित इन्टरनेट दिवस २०२५ को अवसरमा राष्ट्रिय स्तरको वेबिनार आयोजना गरियो। नेपाल दूरसञ्चार प्राधिकरणको संयोजनमा सञ्चार तथा सूचना प्रविधि मन्त्रालय, महिला, बालबालिका तथा ज्येष्ठ नागरिक मन्त्रालय र राष्ट्रिय बाल अधिकार परिषद्को आयोजना तथा नेट फर गुड एलाइन्स, क्रिएसन सोसाइटी नेपाल र जोइनिड फोर्सेस नेपालसँगको सहकार्यमा कार्यक्रम आयोजना गरिएको थियो। कार्यक्रममा बालबालिका तथा अनलाइन सुरक्षा सम्बन्धी विभिन्न संस्थाका विज्ञहरू नेपाल दूरसञ्चार प्राधिकरण (श्री विजय कुमार राय), राष्ट्रिय साइबर सुरक्षा केन्द्र (श्री राजकुमार महर्जन), नेपाल प्रहरीको साइबर ब्यूरो (श्री उमेश प्रसाद शाह) र महान्यायाधिवक्ताको कार्यालय (श्री बिना दाहाल) लगायतले डिजिटल युगमा बालबालिकाको सुरक्षाको महत्त्वबारे प्रस्तुतिकरण गर्नुभएको थियो। कलाकार तथा सञ्चारकर्मी श्री राजा राजेन्द्र पोखरेलले प्यानल छलफल सहित सम्पूर्ण वेबिनारलाई सहजीकरण गर्नुभयो। वेबिनारको क्रममा प्यानल सदस्यहरूले अनलाइन बाल सुरक्षा सम्बन्धी प्रमुख नीतिहरू, अभ्यासहरू र तत्कालिन सवालहरूका साथै अनलाइन सुरक्षाका कानुनी पक्षहरूबारे आफ्ना विचारहरू राख्नुभएको थियो। प्यानल सदस्यहरूले अनलाइन बाल सुरक्षा सम्बन्धी केही घटनाहरू र प्रमाणहरू पनि प्रस्तुत गर्नुभयो। प्यानल छलफलमा सहभागी बालबालिकाहरूले उठाएका केही जिज्ञासाहरूको सम्बन्धित प्यानल सदस्यहरूले जवाफ दिनुभयो। अन्त्यमा, राष्ट्रिय बाल अधिकार परिषद् (राम बहादुर चन्द) सहित सम्बन्धित सरोकारवालाहरूले केही मुख्य सन्देशहरू प्रस्तुत गर्नुभएको थियो र महिला, बालबालिका तथा ज्येष्ठ नागरिक मन्त्रालयका सह-सचिव श्री चक्रबहादुर बुढाको समापन मन्तव्यसँगै सत्र समापन भएको थियो।

सुरक्षित इन्टरनेटका लागि सरकार र सेवा प्रदायकहरूको भूमिका सम्बन्धी राष्ट्रिय कार्यशाला: नेपाल दूरसञ्चार प्राधिकरणबाट सम्बन्धित मन्त्रालयहरू, नियामक निकायहरू र नागरिक समाजका साझेदारहरूको सहकार्यमा आयोजित यस कार्यशालामा नेपालका बढ्दो साइबर चुनौतीहरूलाई सम्बोधन गर्न १४४ जना सहभागीहरूको सहभागितामा राष्ट्रिय कार्यशाला सम्पन्न भयो। इन्टरनेट सेवा प्रदायक संघ, एनसेल आजियाटा लिमिटेड तथा नेपाल दूरसञ्चार कम्पनी लिमिटेडका प्रतिनिधिहरूले डाटा चुहावट र ट्रन्याकिड जस्ता जोखिमहरू विरुद्ध लड्ने प्रयासहरूलाई प्रकाश पार्नुभएको थियो। नेपाल राष्ट्र बैंकको प्रतिनिधिबाट डिजिटल वित्तीय नियमनसम्बन्धी नीतिगत व्यवस्थाहरू तथा योजना प्रस्तुत भएको थियो। नेपाल प्रहरी, साइबर ब्यूरोका प्रतिनिधिबाट महिला तथा बालबालिका सम्बन्धी २०,००० भन्दा बढी घटनाहरू घटेको, साथै साइबर अपराधका शृंखला तथा प्रवृत्तिहरूको बारेमा संक्षिप्त प्रस्तुतिकरण गरिएको थियो। स्रोतसाधनको कमी, अन्तरदेशीय समन्वय र फरेन्सिक क्षमताहरूमा रहेका कमीहरूलाई समेत औल्याइएको थियो। प्यानल छलफलमा कार्यान्वयनमा रहेका चुनौतीहरूलाई सम्बोधन गर्न सुशासन, सार्वजनिक-निजी साझेदारी

र समावेशी नीति निर्माणमा जोड दिइएको थियो । अतिथिहरूले बाल संरक्षण, जनस्तरमा जागरूकता र नैतिक एआई प्रयोगमा जोड दिए।

समग्रमा साइबर सुरक्षाको लागि सरकारको भूमिका र प्रतिबद्धता साथै सरोकारवालाहरूको डिजिटल सुरक्षा तथा साक्षरता अभियानमा साझेदारितालाई प्राथमिकता दिने र सरकारले सबै पक्षको समन्वयमा नीतिगत सुधार र कार्यान्वयनमा पहलकदमी लिनु पर्ने विषयमा जोड दिइएको थियो । । अनलाइन सुरक्षा सम्बन्धी उजुरी, स्रोतसाधनको अभाव र सुरक्षालाई पहुँचसँग सन्तुलन गर्ने जस्ता चुनौतीहरूको सामना गर्न परिष्कृत प्राविधिक क्षमता, एकीकृत ढाँचाहरू र राष्ट्रव्यापी साइबर हाइजिन पहलहरूको लागि पहलकदमी गर्नुपर्नेमा जोड दिइएको थियो जसले सामूहिक रूपमा नेपालको सुरक्षित डिजिटल इकोसिस्टमलाई अगाडि बढाउने विश्वास गरिएको छ।

Contents

<i>SUMMARY</i>	<i>i</i>
<i>सारांश</i>	<i>ii</i>
1. BACKGROUND	- 1 -
2. APPROACH	- 3 -
2.1 Formation of the Sub-Committee	- 3 -
2.2 Program Design	- 3 -
2.3 Safeguarding Considerations	- 4 -
3. EVENT PROCEEDINGS	- 5 -
3.1 Event 1: Webinar on Child Online Safety	- 5 -
3.1.1 Event Overview.....	- 5 -
3.1.2 Objectives.....	- 5 -
3.1.3 Key Sessions & Discussions	- 6 -
3.1.4 Event Outcomes	- 11 -
3.1.5 Key Recommendations	- 12 -
3.2 Event 2: National Workshop on the Role of Government and Service Providers for Safer internet	- 13 -
3.2.1 Event Overview.....	- 13 -
3.2.2 Objectives.....	- 13 -
3.2.3 Key Sessions & Discussions	- 13 -
3.2.4 Outcomes	- 19 -
3.2.5 Recommendations	- 20 -
7. CONCLUSION	- 21 -
8. Appendices	- 22 -
Appendix A: Pictorial Highlights	- 23 -
Appendix B: Greetings messages	- 24 -
Appendix C: Children Responses and feedback	- 29 -

1. BACKGROUND

The digital revolution has transformed societies globally, offering unprecedented opportunities while introducing significant challenges. Safer Internet Day (SID) is an international event initiative celebrated yearly to promote safe and responsible internet use. It is especially designed to encourage proper use of online technology and mobile devices among children and young people. Originating from Europe, SID has grown into a global initiative followed over more than 170 countries. The theme for 2025 is 'together for better internet'. Safer Internet Day (SID), celebrated annually, is a global initiative aimed at promoting the safe and responsible use of digital technologies. This year's SID, observed on February 11, 2025, under the theme "Together for a Better Internet," emphasized collective responsibility in fostering a secure and inclusive digital environment.¹

In modern day's era of digital transformation, children are the most vulnerable to the internet. It is used in education, entertainment, and many other social infrastructures in their daily life. This has made them vulnerable to the influence of online abuse, cyberbullying, internet exploitation, and exposure to inappropriate content. Safer Internet Day serves as a reminder and an important platform to address these issues, create awareness, and provide tools to promote safe online practices.

In Nepal, the increasing penetration of internet services has brought both opportunities and risks. While digital technologies have enhanced communication, education, and economic activities, they have also exposed users to cyber threats such as online exploitation, misinformation, and privacy breaches.² Recognizing these challenges, the Nepal Telecommunications Authority (NTA), in collaboration with the Ministry of Communication and Information Technology (MoCIT), Ministry of Women, Children and Senior Citizens (MoWCSC), National Child Rights Council (NCRC), and other stakeholders, organized a comprehensive program to mark SID 2025.³

The SID 2025 program in Nepal highlighted the importance of digital literacy as a tool for empowerment. By equipping individuals with the knowledge and skills to navigate the digital world safely, the initiative contributed to building a resilient digital society. It also underscored the need for continuous efforts to address emerging cyber threats and to promote a culture of responsible digital citizenship.⁴ Collaboration among multiple stakeholders was a cornerstone of the initiative. By engaging government bodies, non-governmental organizations, educators, parents, and the private sector, the program fostered a multi-stakeholder approach to addressing

¹ Better Internet for Kids. (2025). Safer Internet Day 2025: Local initiatives drive global impact.

² ChildSafeNet. (2025). Child online safety Nepal: Safer Internet Day 2025.

³ Ministry of Women, Children and Senior Citizens. (2025). National Child Rights Council public information tabloid.

⁴ Kaspersky. (2025). Top 15 internet safety rules and what not to do online.

internet safety challenges. This approach not only enhanced the program's reach but also ensured the sustainability of its outcomes.

The program aimed to raise awareness about online safety, particularly among children and youth, who are most vulnerable to cyber risks. Activities included awareness webinar, capacity-building workshop, and interactive session designed to educate participants on safe online practices. These efforts aligned with the objectives of the Digital Nepal Framework, which emphasizes digital literacy and cybersecurity as key components of the nation's digital transformation.⁵

⁵ ICT Frame. (2025). Digital Nepal Framework 2.0: A step towards a digitally empowered Nepal.

2. APPROACH

The Safer Internet Day 2025 initiative was designed as a collaborative effort involving key government agencies, law enforcement bodies, civil society organizations, and child rights stakeholders to promote a safe digital environment for children. The Nepal Telecommunications Authority (NTA), in coordination with the Ministry of Communication, Information and Technology (MoCIT), the Ministry of Women, Children, and Senior Citizens (MoWCSC), the Cyber Bureau of Nepal Police, the National Child Rights Council (NCRC), and civil society organizations such as Joining Forces, Net4Good Alliance, and Creation Society Nepal, led the strategic planning and execution of the event.

2.1 Formation of the Sub-Committee

NTA formed a sub-committee, comprising the following representatives from key institutions to ensure structured, meaningful and impactful events on the occasion of SID 2025. The committee was responsible for designing the program structure, identifying speakers and panelists, selecting discussion themes, organising events and preparing reports ensuring safeguarding protocols were in place.

- | | |
|---|-------------------|
| a. Mr. Bijay Kumar Roy, Director, NTA | - Co-ordinator |
| b. Ms. Roja Kiran Basukala, Deputy Director, NTA | - Member |
| c. Mr. Ram Bahadur Chand, Officer/Information Officer, NCRC | - Member |
| d. Ms. Kamala Dahal, Officer, MoCWSC | -Member |
| e. Mr. Saurav Lamsal, Officer, MoCIT | -Member |
| f. Mr. Biwek Nath Mahaseth, Assistant Director, NTA | -Member |
| g. Mr. Krishna Bahadur Karki, Assistant Director, NTA | -Member Secretary |

2.2 Program Design

The event was structured into two key sessions to maximize outreach and effectiveness:

1. **Keeping Children Safe on Internet: A Webinar on Child Online Protection**
 - o A two-hour interactive webinar tailored for children to raise awareness on safer internet practices.
 - o Conducted via Zoom with a live broadcast on Facebook and YouTube pages of Joining Forces Nepal member organizations.
 - o **Engagement tools:** A survey link was shared in the Zoom chat to collect feedback on children's online experiences.

- **Facilitator:** Raja Rajendra Pokhrel, a journalist and artist, led the session.
- **Key Messages:** Delivered by representatives from NTA, ITU Area Office and Innovation Centre for South Asia, Cyber Bureau, National Cyber Security Center (NCSC), Office of Attorney General, MoWCSC, and civil society organizations working on child online safety. Participating children also shared their experiences and perspectives.

2. Government and Stakeholder Dialogue on Safer Internet

- A high-level policy discussion focusing on the role of government and stakeholders in ensuring a safer internet.
- **Program Facilitator:** Roja Kiran Basukala, Deputy Director, NTA.
- **Chairperson:** NTA Chairman.
- **Chief Guest:** Hon. Prithvi Subba Gurung, Minister, MoCIT.
- **Guest Speakers:**
 - Bam Bahadur Baniya, Vice Chairperson, NCRC
 - Radhika Aryal, Secretary, MoCIT
 - Laxmi Kumari Basnet, Secretary, MoWCSC
 - Indira Devi Dhakal, Member Secretary, NCRC
 - Nawaraj Dhakal, Co-ordinator, Net4Good Alliance
 - Dr. Ganga Bahadur Gurung, Joining Forces
- Program Structure:
 - Presentation on cybersecurity policies and digital safety initiatives.
 - Panel Discussion featuring experts from government, civil society, and law enforcement.

2.3 Safeguarding Considerations

To ensure a safe and inclusive environment, particularly for children, strict safeguarding measures were implemented:

- Pre-registration requirement for participants to prevent unauthorized access.
- Moderation of children's contributions to protect their identities and well-being.
- Regulated participation to prevent any potential online risks.
- Real-time moderation of online comments and questions to ensure respectful discourse.

3. EVENT PROCEEDINGS

3.1 Event 1: Webinar on Child Online Safety

3.1.1 Event Overview

Date: 11 February 2025

Time: 11:00 AM to 01:00 PM (2 Hours)

Platform: In-Person/Zoom/YouTube/Facebook

Participants: Diverse forms of participants (In-person and Online) have participated in the webinar via a Zoom platform, and also from different social media live streaming (Facebook and YouTube), which are as follows,

S. N.	Participants Numbers	Medium	Description
1	40+	In-Person	Organizing committee members, collaborating and partners organization members, Supporters, Guests, panelists, moderators, and Technical team members were physically presented at the program venue.
2	400+ zoom connections connecting 2,000+ individuals	Zoom Platform	432 accounts were connected to a Zoom platform. In most accounts that were joined from schools, a group of students, a whole classroom, or whole students also participated in the program via a single connection.
3	10,000+	Facebook Live Streaming	The webinar was live-streamed via different organizers and supporters' Facebook pages. The webinars were live-streamed by 10+ partnering organizations Facebook pages and got 10K+ views.
4	1000+	YouTube Streaming	The webinar live streaming and post video was also shared on YouTube and got 1K plus views.
	13,000+	Total	Approximately

3.1.2 Objectives

The major objectives of the program are as follows:

- To highlight the importance of safer internet day for children and identify specific challenges.

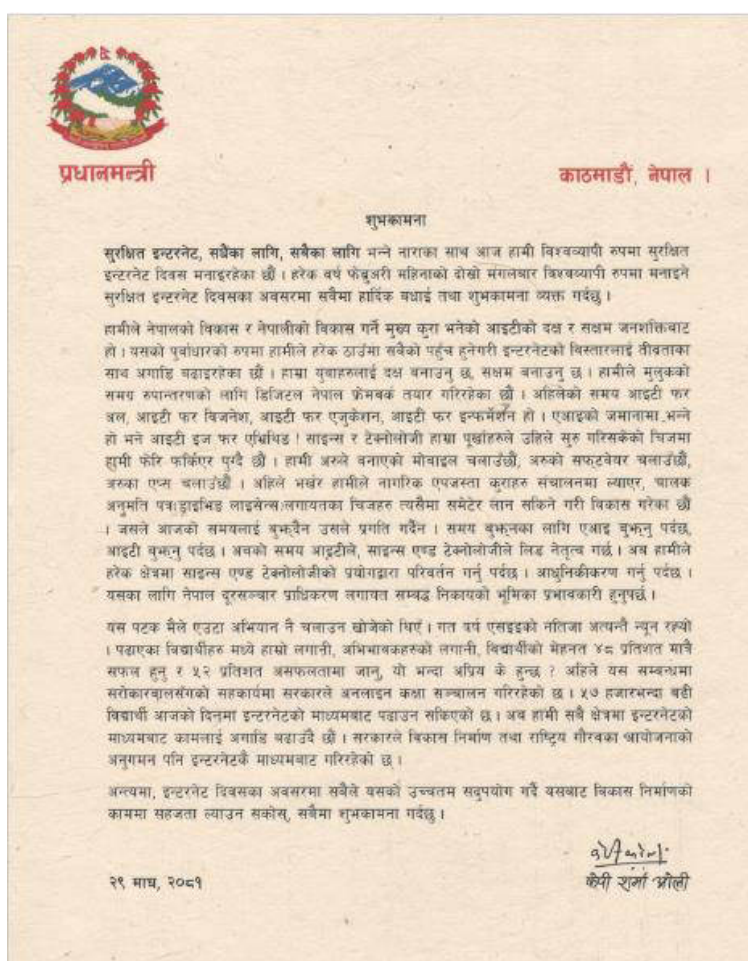
- To share and disseminate internet-borne risks and impact on children and practices of existing safety measures
- To gather insights and opinions from key stakeholders including telecommunications authorities, children, government agencies, and UN agencies, for protection on online platforms



3.1.3 Key Sessions & Discussions

Opening, Welcoming, and Messages

The webinar was started with a key message from the Right Honorable Prime Minister K.P. Sharma Oli, which highlighted the importance of online learning and information in education.



International Telecommunications Union (ITU) Area Office and Innovation Centre for South Asia- Dr. Pranita Upadhyaya, gave a brief speech and showed the importance of government

and service providers in creating a safer, more secure digital environment. She highlighted Internet has become deeply embedded in our life. While it is convenient to use, it brings risk in our privacy and security online. Government and service providers are key players in developing and implementing policies, frameworks and technologies to make sure internet is a safe space for all, especially children and vulnerable groups.

The webinar featured panel members who presented their findings and created a discussion about children in online spaces. These panel members providing presentation included:

- Bijay Kumar Roy, Director, NTA
- Umesh Prasad Sah, DSP, Cyber Bureau, Nepal Police
- Raj Kumar Maharjan, Director, National Cyber Security Center,
- Bina Dahal, Deputy Attorney, Office of the Attorney General



Panel Members Presentation

Bijay Kumar Roy, Director of the Nepal Telecommunications Authority (NTA), delivered a presentation on Cybersecurity Policies and Online Protection Initiatives. His session provided essential insights into cybersecurity, emphasizing its significance in safeguarding digital assets and personal data from theft, misuse, and damage.

Roy elaborated on the various online dangers that pose significant threats, particularly to children. These include child grooming, cyberbullying, sexting, sextortion, child pornography, online gaming addiction. He underscored the importance of educating individuals on the safe use of digital platforms such as Facebook, Instagram, X, LinkedIn, and WhatsApp, as a lack of awareness can expose users to security risks.



The presentation also covered Nepal's regulatory framework for cybersecurity, outlining key legal provisions established by the government to address online safety. Notable regulatory frameworks include Child Online Protection Guideline (2019), Cyber Security Byelaw (2020), National Cyber Security Policy (2023) and Nepal's position in Global Cyber Security Index published by ITU. Roy referenced the ITU Council Resolution 1305, which identifies

cybersecurity as a critical global policy issue to ensure safe, equitable, and reliable access to digital services.

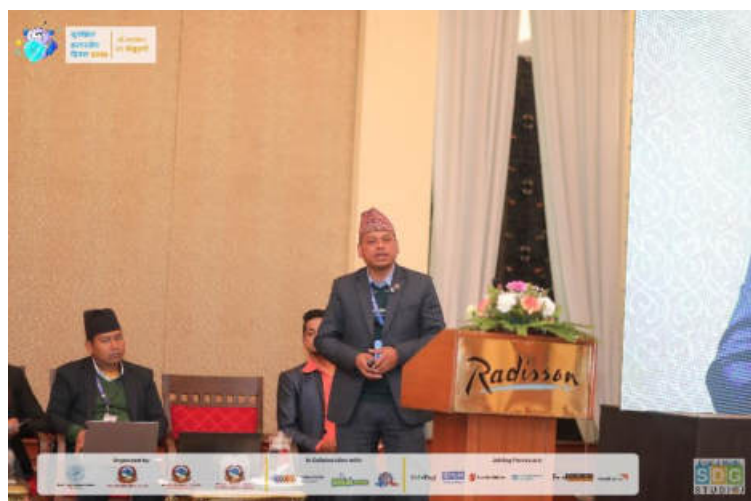
Other NTA initiatives such as Cyber Security Awareness Assessment Report (2015) and Child Online Protection (COP) awareness programs and Training of Trainers (ToT), Net4Good Manual, cyber security advisories to the general public and provincial policy discussion and awareness were conducted in collaboration with international and national support partners.

As a way forward, Roy emphasized the need for effective implementation of existing laws, development of educational policies, and enhanced institutional frameworks. He called for greater coordination among government agencies and stakeholders to conduct awareness programs, ensuring accountability at central, provincial, and local levels. Strengthening cybersecurity efforts through collaboration with media, social organizations, and policymakers will be essential in building a safer digital environment for all.

During the session, DSP Umesh Prasad Sah from the Cyber Bureau, Nepal Police delivered a presentation on “Cyber Threats and Child Online Abuse Cases.” His discussion shed light on the increasing risks children face in digital spaces, particularly emphasizing that girls are disproportionately targeted and subjected to cyber abuse compared to boys. He illustrated various cybercrime scenarios, providing real-world cases to highlight the growing concerns surrounding child exploitation online.

DSP Sah outlined several prevalent forms of cyber abuse affecting children. He detailed cases where perpetrators create fake identities to send threatening messages, engage in verbal abuse, defame individuals, or blackmail victims. Additionally, social media platforms have increasingly been misused as tools for personal revenge or expressing anger, often leading to harassment and intimidation. Another critical issue is digital image manipulation, where offenders extract photos from victims’ social media accounts, alter them (e.g., superimposing a victim’s face onto explicit content), and use these doctored images for harassment, coercion, or public humiliation. In some cases, victims are threatened with the viral dissemination of explicit content, pressured into non-consensual relationships, or coerced into inappropriate video interactions.

The presentation also covered incidents where offenders secretly record or fabricate explicit images/videos with the intent of financial exploitation, entertainment, or revenge, subsequently sharing such content in online groups. A particularly alarming trend involves social media friendships with strangers, which perpetrators exploit to harass victims by sending inappropriate videos.



Furthermore, cases have been reported where offenders specifically target students and teachers with explicit material or even impersonate cyber law enforcement officials to pressure victims into sharing sensitive content.

Statistical insights provided by DSP Sah revealed that the most common cybercrime cases involving child victims relate to hacking and fake accounts, while cyber tip-line reports constitute the lowest percentage. The data further indicated that Facebook, Messenger, WhatsApp, Instagram, TikTok, and E-Sewa are the primary platforms through which cybercrimes are committed. In terms of demographic trends, individuals aged 36-50 are the most vulnerable victims of cybercrimes, while offenders generally fall within the 19-25 age group.

To illustrate the severity of these crimes, DSP Sah shared brief case studies of real incidents. In one case, a 21-year-old woman from Bhaktapur was found guilty of exploiting her 14-year-old sister by recording and sharing explicit footage with her boyfriend. This case was escalated to the District Police Office, Bhaktapur. In another shocking instance, an 8-year-old boy from Jhapa was discovered to have recorded and uploaded his own nude video to YouTube. Another severe case involved a 23-year-old man from Nawalparasi who filmed an 11-year-old girl, capturing explicit images of her genitalia, with disturbing content suggestive of child exploitation.

These findings underscore the urgent need for enhanced cybercrime prevention strategies, stricter legal enforcement, and greater digital literacy initiatives to safeguard children from online threats. Strengthening awareness campaigns, parental supervision, and technical monitoring measures is imperative to combat these emerging forms of cyber abuse.

During the session, Raj Kumar Maharjan, Director of the National Cyber Security

Center, delivered a presentation on “How Can We Safely Use the Internet?” His discussion highlighted the legal frameworks established to promote online safety and the role of the National Cyber Security Center in preventing and addressing online abuse. He emphasized the increasing digital risks faced by internet users, particularly children and young people, and outlined measures to enhance cybersecurity and online safety.



The internet, as a vast global network of interconnected devices, serves as the backbone of modern communication, facilitating information exchange, social interactions, and economic activities. However, the growing dependence on digital platforms has also exposed users, particularly children, to cyber threats. The impact of COVID-19 lockdowns significantly

increased internet usage, with studies revealing that one in four children and young people (25%) spent over ten hours online daily.

One of the most concerning aspects of digital risks is Online Child Sexual Exploitation (OCSE), which involves the manipulation and coercion of children into sexual activities. OCSE includes various forms of abuse, such as grooming, online sexual exploitation, child pornography, and sexting. These activities not only have severe psychological and emotional consequences for victims but also pose a significant challenge for law enforcement agencies in identifying and addressing such crimes.

To mitigate these risks and ensure a safe online environment, the National Cyber Security Center has implemented several policies and monitoring mechanisms. These include mandatory registration of social media platforms, the establishment of a Point of Contact (POC) system, the introduction of Cyber Security Advisory services, and the formulation of an AI and Data Protection Policy. These measures aim to strengthen cyber resilience, protect digital identities, and safeguard users from emerging cyber threats.

The Cyber Security Advisory, which was officially launched on Magh 8, 2081 B.S., plays a crucial role in enhancing cybersecurity across various sectors. It provides guidance on government website and application security, server and network protection, device security, password management, and safe internet browsing practices. Additionally, it addresses phishing attacks, email security, social media safety, mobile security, and the responsible use of removable media. These comprehensive strategies aim to create a robust digital infrastructure, ensuring a secure online environment for individuals, organizations, and government entities.

Deputy Attorney, Bina Dahal gave insights into the rights of children and their responsibility as well through her topic 'Legal Framework for Child Online Protection'. She presented acts related to children such as: Child Related Act 2075, Online Child Protection Guidelines 2076, National Penal Code 2074. She put light into the rights of children and how they can use it. Any abuse done towards any child will be punished at minimum of 4 years and 1,00,000 fines.



Children Participants

Children from various regions of Nepal actively participated in the webinar, raising concerns about online safety, cybersecurity risks, and limited internet access in rural areas. They emphasized the need for a national policy to address excessive internet usage among youth and

inquired about the government's efforts to combat cybercrime and protect children online. Participants also highlighted gaps in implementing existing cybersecurity laws and the lack of digital literacy programs in schools.

In response, experts from the Nepal Telecommunications Authority (NTA) outlined ongoing initiatives, including broadband expansion in schools and the integration of cybersecurity topics into the curriculum. They stressed the importance of parental supervision, community awareness, and proactive reporting of online threats. The discussion underscored the need for multi-level engagement, legal enforcement, and cross-border collaboration to enhance cybersecurity and ensure a safer digital space for children.



3.1.4 Event Outcomes

- Highlighted the importance of internet safety to 2000+ children and emphasized to overcome challenges.
- Disseminated information regarding internet-borne risks and its impact on children.
- Shared different practices for online safety measures.
- Discussed and shared insights and opinions of key stakeholders including regulators, children, government agencies, and UN agencies, for protection on online platforms.
- Sensitized stakeholders to execute their roles and responsibilities underscoring the critical roles of government to ensure online safety and security.
- Provided a platform for various stakeholders to present findings and discuss the specific challenges children face online.
- Demonstrated a successful collaborative effort between government agencies, civil societies and development partners to reach a nationwide audience on online safety.

At the end of the session, key outcomes of the workshop were shared. The webinar concluded with a speech and thanks done by Chakra Bahadur Budha- Joint Secretary, MoWCSC. With the joint effort of Nepal Government agencies and JF Nepal, the webinar reached all across the nation and concluded successfully.



3.1.5 Key Recommendations

- Ensure effective enforcement of existing frameworks like Child Online Protection Guideline, 2019, Cyber Security Byelaw (2020) and National Cyber Security Policy (2023).
- Develop and implement age-appropriate modules on cybersecurity, ethical internet use, and online risk prevention.
- Work in close collaboration and co-operation with government, civil societies, internet service providers, cyber security entities, influencers, and local media to run campaigns on child online protection.
- Develop Curriculum for safer internet practices for children.
- Conduct capacity building programs for school teachers, parents, trainers and local governments to reduce the risks of online vulnerabilities and threats.
- Host regular forums where children share their online experiences to shape child-centric policies and reporting mechanisms.
- Co-ordinate and collaborate with concerned national and international agencies to minimize cross-border cybercrimes.

3.2 Event 2: National Workshop on the Role of Government and Service Providers for Safer internet

3.2.1 Event Overview

- **Date:** 11 February 2025
- **Venue:** Hotel Radission, Kathmandu, Nepal
- **Participants:** 144 in total
- **Organizers**

The NTA continued its collaborative efforts, partnering with the MoCIT, MoWCSC, NCRC, Net4Good Alliance, World Vision International, Plan International, SOS Children's Villages, Terre des Hommes, Child Fund Japan, Save the Children, and Creation Society Nepal for this workshop.



3.2.2 Objectives

The National Workshop aimed to bring together key stakeholders from the government and service provider sectors to discuss their respective roles and responsibilities in promoting a safer internet environment in Nepal.

3.2.3 Key Sessions & Discussions

The workshop was facilitated by Ms. Roja Kiran Basukala, Deputy Director, Nepal Telecommunication Authority.

The workshop commenced with formal welcome remarks by Mr. Bijay Kumar Roy, Director of NTA. He emphasized NTA's commitment to promoting safer internet practices in Nepal, with a specific focus on the well-being of children and marginalized communities. Mr. Roy welcomed all the participants and set the stage for the day's discussions.

The inauguration of the workshop was conducted by the Chief Guest, the Honorable Minister of the Ministry of Communication and Information Technology (MoCIT), Mr. Prithvi Subba Gurung. The inauguration was followed by the recitation of the National Anthem.



Following the inauguration, well-wishes messages from several high-ranking officials were displayed, including the Prime Minister of Nepal, the Ministry of MoCIT, the Secretary of MoCIT, the Ministry of Women, Children and Senior Citizens (MoWCSC), and the Chairman of the NTA. These messages underscored the national importance of internet safety and the collaborative efforts required to achieve it.

Dr. Pranita Upadhyaya, Head of the ITU Regional Office for South Asia and Innovation, conveyed a message of support from the International Telecommunication Union (ITU). She acknowledged the immense opportunities presented by internet technology for development and innovation while also highlighting the significant security, safety, and privacy threats that arise in the digital space. Dr. Upadhyaya affirmed ITU's commitment to introducing frameworks and guidelines aimed at ensuring the safety and privacy of individuals online and expressed the organization's readiness for future collaboration with Nepal.

a) Policy Provisions and Initiatives for Cyber Security:

Mr. Narayan Timilsina, Joint Secretary of MoCIT, delivered a presentation focusing on the policy provisions and initiatives for cyber security in Nepal. He highlighted the Cyber Security Policy 2080, which prioritizes the safety and security of individuals and institutions, with the overarching goal of ensuring a secure cyberspace in alignment with the Global Cybersecurity Index (GCI) indicators. Mr. Timilsina informed the audience about the drafting of a new Cyber Security Bill and the formation of key national bodies, including the National Cyber Security Center, the Cyber Security Advisory Group, and the Critical Information Infrastructure Identification (CII) framework. He also outlined plans under the Digital Nepal Project to promote the Security Operations Center (SOC), Network Operations Center (NOC), and digital forensics and cyber infrastructure, while also emphasizing the future importance of quantum computing, Artificial Intelligence (AI), and 5G technologies in the cybersecurity landscape.



b) Online Safety Practices and Security Measures:

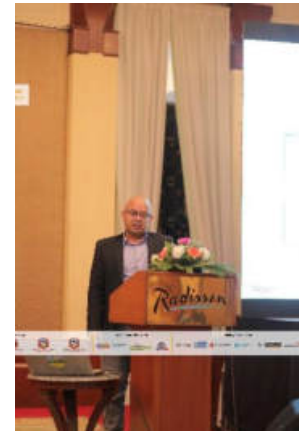
Mr. Ram Krishna Pariyar, representing the Internet Service Providers Association of Nepal (ISPAN), presented on Online Safety Practices and Security Measures. He shared crucial insights into the current security measures being implemented by the internet service providers. Mr. Pariyar stated that Nepal is highly vulnerable to cyber threats and highlighted the risks associated with leaking sensitive information online, such as operating system details, browser information, hardware specifications, location data, passwords, auto-fill information, and personal data. He also discussed tracking mechanisms like browser fingerprinting and tracking advertisements. To enhance online safety, Mr. Pariyar recommended utilizing "do not track" options, being cautious about sharing credentials and personal information, practicing critical thinking before clicking on links, and implementing robust security strategies such as endpoint protection and



open-source intelligence. He mentioned that ISPAN is actively conducting awareness campaigns to promote these practices.

c) Security Governance by Telecommunication Service Providers:

Mr. Rajesh Lal Nyachhyon from Ncell, a telecommunication service provider, focused his presentation on security governance within the telecom sector. He explained that Ncell is prioritizing cyber security maturity in line with the NTA Cyber Security Bylaw 2020 and is pursuing ISO 20001 Information Security Management System (ISMS) certification. Mr. Nyachhyon also emphasized Ncell's commitment to data privacy, including data governance, breach management protocols, and awareness programs. He expressed Ncell's openness to collaborate with various stakeholders to strengthen the overall online safety ecosystem.



d) Regulation for Digital Financial Services Security:

Mr. Krishna Ram Dhoju, Director at Nepal Rastra Bank (NRB), delivered a presentation on the Regulation for Digital Financial Services (DFS) Security in Nepal. He began by highlighting the importance and opportunities presented by the rapidly growing digital financial services sector in Nepal over the past decade. Mr. Dhoju then presented the regulatory framework and security measures implemented by NRB in this domain. He stated that strengthening DFS is a high priority for NRB, and recent initiatives include the planned development of a Central Bank Digital Currency (CBDC) as a Digital Public Infrastructure (DPI) to further support DFS. He also mentioned the government's Digital Nepal Framework 2019 and NRB's formulation of the Payment System Rated Unified Directives 2080 and Cyber Resilience Guidelines 2023. Furthermore, NRB is actively promoting digital literacy programs to empower users of DFS. Mr. Dhoju also outlined challenges in the DFS sector, including digital financial literacy gaps, cyber security threats, data protection concerns, the need for upskilling stakeholders, inter-regulatory coordination, and regulating FinTech companies. He concluded by highlighting the future opportunities for a resilient and secure digital economy in Nepal.



e) Facts and Figures of Cyber Crime in Nepal:

Ms. Dipa Bhattarai, Inspector from the Cyber Bureau of Nepal Police, presented compelling Facts and Figures about the current state of Cybercrime in Nepal. She highlighted that children and women are particularly vulnerable and are often the primary targets of cybercriminals. The most common reported cases include Child Sexual Abuse Material (CSAM), bullying, extortion, hacking, impersonation, phishing, and financial fraud, with the majority of reported

incidents originating from platforms like Facebook, Instagram, TikTok, WhatsApp, and eSewa. Ms. Bhattarai noted an exponential increase in reported cybercrime cases, with nearly 20,000 cases registered in the last fiscal year, predominantly affecting children and women. She suggested the importance of practicing good cyber hygiene and presented some real-world case examples. Ms. Bhattarai also outlined challenges faced by the Cyber Bureau, including the 35-day timeline for submitting cases to court, the absence of Mutual Legal Assistance Treaties (MLATs) with certain platforms and countries, resource limitations, delays in receiving data from online platforms, a lack of comprehensive data analysis and research capabilities, and issues related to cross-border cybercrime.



f) Policy and Implementation Gaps in Context of Nepal:

Mr. Bibek Rana, a Cyber Security Expert, provided an insightful analysis of the policy and implementation gaps in the context of Nepal. He argued that policy insights are often driven by academics and politicians with limited public voice opportunities, and that policy-making is largely led by bureaucrats. He also pointed out a need to better consider the global context and best practices in internet policy, particularly concerning contemporary issues like AI. Mr. Rana identified several key gaps, including unclear policies, a reluctance towards robust implementation, a lack of effective project management practices, and insufficient participatory approaches in policy development. He emphasized that these gaps make children and young people particularly vulnerable to online threats.



g) Panel Discussion and QA Session:

A comprehensive panel discussion and question-and-answer session was moderated by Mr. Rajan Lamsal. The panel comprised Mr. Bibek Rana, Ms. Dipa Bhattarai, Mr. Krishna Prasad



Bhandari (Manager, Nepal Telecom - NTC), Mr. Krishna Ram Dhoju, and Mr. Narayan Timalisina.

- **Mr. Rana** reiterated the need for strategies to increase public participation in policy-making and emphasized a more structured framework rather than ad-hoc approaches.
- **Ms. Bhattarai** stressed the importance of registering social media accounts for accountability, along with the need for increased resources and enhanced cyber forensics capabilities within the Cyber Bureau.
- **Mr. Bhandari (NTC)** stated that while their previous focus was on accessibility, NTC is now prioritizing system security and end-user safety. He acknowledged the challenges faced by service providers in balancing security and competitiveness.
- **Mr. Dhoju (NRB)** outlined plans to develop a resilient DFS system covering digital wallets and transactions, noting the current limitation to banks and financial institutions. He identified the lack of public awareness as a major issue in DFS and affirmed NRB's responsibility to strengthen institutions, mentioning the provision of tracking and response mechanisms.
- **Mr. Timalisina (MoCIT)** acknowledged the implementation gaps due to resource constraints and stated that plans are underway to incorporate these issues in upcoming policies, including increasing specialized IT human resources and updating the Digital Nepal Framework to enhance digital infrastructure.



The Q&A session focused on key challenges in cybersecurity, including coordination among service providers, gaps in human resources and legal frameworks, and the roles of civil society and government in law enforcement. Discussions emphasized the importance of a collaborative approach rather than isolated efforts, highlighting the need for inclusive participation of children, women, and vulnerable groups. Concerns were also raised about challenges in accessing data. Panelists acknowledged these issues and expressed commitment to future collaboration to enhance



h) Remarks by Guests and Speakers

Mr. Nawaraj Dhakal from Net4Good Alliance emphasized the safety, access, approach, and protection of children online and welcomed collaboration from all stakeholders. Dr. Ganga Bahadur Gurung from Joining Forces highlighted the importance of multi-stakeholder collaboration for protecting vulnerable children online.

Ms. Laxmi Kumari Basnet, Secretary of MoWCSC, highlighted the increased importance of internet facilities during post-COVID-19 in education, communication, and skills development. However, she also noted its impact on social behavior and the rise in crime, with children and women being particularly vulnerable. Ms. Basnet pointed out the discrepancy between reported cases and actual incidents and emphasized the need for collaborative efforts in awareness and capacity building, especially concerning issues like child marriage and trafficking exacerbated by the internet.



Ms. Radhika Aryal, Secretary of MoCIT, acknowledged the exponential increase in internet penetration globally and nationally. She mentioned the government's efforts to deliver services through online platforms, which while increasing access, has also elevated vulnerabilities. Ms. Aryal appreciated all the suggestions and comments, noting that the government sector itself is increasingly targeted by hackers and attacks. She highlighted initiatives by MoCIT, including plans to increase connectivity and digital service delivery systems, and mentioned that social media registration is in process. Ms. Aryal requested all regulatory and service delivery agencies to focus on effective monitoring and quality assurance and committed to working collaboratively.



Mr. Bam Bahadur Baniya, Vice Chairman of the National Child Rights Council, stated that the misuse of the internet and internet services is increasing exponentially. He informed the audience that NCRC is promoting child protection mechanisms at federal, provincial, and local levels, emphasizing that key safety messages should reach the grassroots level. Mr. Baniya mentioned NCRC's plans to strengthen helplines 104 and 1098 and appreciated this collaboration and anticipated furthermore similar partnership in near future.



i) Address by the Chief Guest:

The Honorable Minister of MoCIT, Mr. Prithvi Subba Gurung, emphasized the importance of information, communication, science, and technology for socio-economic development of country. Minister Gurung stated that effective implementation of laws and policies is required. He appreciated the efforts of NTA and expressed a desire to prioritize innovation in ICT sector. He highlighted the government's priorities in human resource development, need of increased investment in the ICT sector, and formulation of necessary regulations for cyber security. The Minister affirmed the government's role in ensuring the right to information, data privacy and management, and controlling the misuse of social media. He also acknowledged the pros and cons of AI, emphasizing the importance of promoting ethical use of AI for social good. He focused on a larger digital literacy campaign, digital infrastructure development and balanced private sector involvement for safer internet in Nepal.



j) Closing:

The Program Chair, Mr. Bhupendra Bhandari, Chairman of NTA, expressed his expectation for greater support of stakeholders and collaboration in the future for safer internet in Nepal. He appreciated active and remote participation of thousands of children from various schools of different provinces and successful completion of the webinar held on the occasion of safer internet day 2025. He summarized the key points of the presentations made by the presenters and panel discussions of the workshop. He thanked all the service providers and partner organizations for their participation and made commitment for future collaborations.



3.2.4 Outcomes

- Active participation and contribution of the key stakeholders from the government, civil societies, private sectors, partnering organizations and service providers towards performing their roles and responsibilities for promoting a safer internet environment in Nepal.
- Sensitized roles of government bodies, service providers, civil societies, international agencies towards effective implementation of cyber security policies, online safety practices, regulatory frameworks for online safety.

- Government officials and other stakeholders gained insights into the online safety practices and security measures currently being implemented by internet and telecommunication service providers, including their challenges and future plans.

3.2.5 Recommendations

- Develop comprehensive national child online protection policies/frameworks.
- Build and strengthen Legal and Policy Frameworks for safer internet ecosystem.
- Promote public-private partnerships to develop and implement effective programs to address online safety challenges .
- Launch comprehensive campaigns and programs for online safety and digital literacy including digital financial literacy, targeting vulnerable groups.
- Promote adoption of security standards, strengthen monitoring, explore technical solutions, and improve reporting mechanisms for secure and resilient network infrastructure
- Develop information sharing mechanisms , perform necessary actions and collaborations for safer internet .
- Develop and implement capacity building programs to strengthen expertise in government bodies, regulatory authorities, law enforcement agencies, prosecutors, trainers, educators etc.

7. CONCLUSION

The Safer Internet Day 2025 was celebrated in Kathmandu, Nepal on February 11, 2025. The event was successfully organized by Nepal Telecommunications Authority (NTA), the Ministry of Women, Children and Senior Citizens (MoWCSC), the Ministry of Communication and Information Technology (MoCIT), the National Child Rights Council (NCRC) in collaboration with Joining Forces, Net4Good Alliance and Creation Society Nepal. On this occasion, a webinar was held in the morning session where school children, teachers and relevant stakeholders participated remotely through virtual/online platform. Similarly, a National Workshop was conducted after the webinar which brought diverse stakeholders including government officials, regulators, law enforcement agencies, service providers, and civil society representatives to emphasize their role and responsibilities towards building a safer internet ecosystem.

The discussions and presentations held during these events highlighted the importance of online safety, combating the cyber security threats, data privacy concerns and identified specific vulnerabilities faced by children in the digital space. The active participation and engagement of over 400 accounts connections, 2,000 individuals in the webinar from seven provinces and 144 participants in the national workshop reflected concerns regarding these issues in Nepali society.

In conclusion, the Safer Internet Day 2025 celebrations in Nepal served as a significant milestone in raising awareness, fostering dialogue, and mobilizing collective action towards creating a safer, more secure and responsible online environment for all citizens. The commitment expressed by various stakeholders towards future collaboration and the strengthening of existing mechanisms indicates a positive trajectory for advancing online safety initiatives in Nepal. The continued collaboration and implementation of the insights and recommendations obtained from these programs will be crucial in achieving the goal of "Safe Internet, Forever, For All" in Nepal.

8. Appendices

Appendix A: Pictorial Highlights



Appendix B: Greetings messages

Greetings Message from the [Secretary, Ministry of Communication, Information and Technology.](#)

Greetings Message from the [Chairman, Nepal Telecommunication Authority](#)

Greetings Message from the [Joint Secretary, Ministry of Women, Children and Senior Citizen](#)

Greetings Message from the [Member Secretary, National Child Rights Council](#)

Program videos Youtube Link :

<https://www.youtube.com/watch?v=6-b0AWnSjWo>

<https://www.youtube.com/watch?v=72ERICxI7tE>



प्रधानमन्त्री

काठमाडौं, नेपाल ।

शुभकामना

सुरक्षित इन्टरनेट, सधैंका लागि, सबैका लागि भन्ने नाराका साथ आज हामी विश्वव्यापी रूपमा सुरक्षित इन्टरनेट दिवस मनाइरहेका छौं । हरेक वर्ष फेब्रुअरी महिनाको दोस्रो मंगलबार विश्वव्यापी रूपमा मनाइने सुरक्षित इन्टरनेट दिवसका अवसरमा सबैमा हार्दिक बधाई तथा शुभकामना व्यक्त गर्दछु ।

हामीले नेपालको विकास र नेपालीको विकास गर्ने मुख्य कुरा भनेको आइटीको दक्ष र सक्षम जनशक्तिबाट हो । यसको पुर्वाधारको रूपमा हामीले हरेक ठाउँमा सबैको पहुँच हुनेगरी इन्टरनेटको विस्तारलाई तीव्रताका साथ अगाडि बढाइरहेका छौं । हाम्रा युवाहरूलाई दक्ष बनाउनु छ, सक्षम बनाउनु छ । हामीले मुलुकको समग्र रूपान्तरणको लागि डिजिटल नेपाल फ्रेमवर्क तयार गरिरहेका छौं । अहिलेको समय आइटी फर अल, आइटी फर विजनेस, आइटी फर एजुकेशन, आइटी फर इन्फर्मेशन हो । एआइको जमानामा भन्ने हो भने आइटी इज फर एभ्रिथिङ ! साइन्स र टेक्नोलोजी हाम्रा पूर्खाहरूले उहिले सुरु गरिसकेको चिजमा हामी फेरि फर्किएर पुग्दै छौं । हामी अरुले बनाएको मोबाइल चलाउँछौं, अरुको सफ्टवेयर चलाउँछौं, अरुका एप्स चलाउँछौं । अहिले भर्खर हामीले नागरिक एपजस्ता कुराहरू संचालनमा ल्याएर, चालक अनुमति पत्र(डाइभिड लाइसेन्स)लगायतका चिजहरू त्यसैमा समेटेर लान सकिने गरी विकास गरेका छौं । जसले आजको समयलाई बुझ्दैन उसले प्रगति गर्दैन । समय बुझ्नका लागि एआइ बुझ्नु पर्दछ, आइटी बुझ्नु पर्दछ । अबको समय आइटीले, साइन्स एण्ड टेक्नोलोजीले लिड नेतृत्व गर्छ । अब हामीले हरेक क्षेत्रमा साइन्स एण्ड टेक्नोलोजीको प्रयोगद्वारा परिवर्तन गर्नु पर्दछ । आधुनिकीकरण गर्नु पर्दछ । यसका लागि नेपाल दूरसञ्चार प्राधिकरण लगायत सम्बद्ध निकायको भूमिका प्रभावकारी हुनुपर्छ ।

यस पटक मैले एउटा अभियान नै चलाउन खोजेको थिएँ । गत वर्ष एसइइको नतिजा अत्यन्तै न्यून रह्यो । पढाएका विद्यार्थीहरू मध्ये हाम्रो लगानी, अभिभावकहरूको लगानी, विद्यार्थीको मेहनत ४८ प्रतिशत मात्रै सफल हुनु र ५२ प्रतिशत असफलतामा जानु, यो भन्दा अप्रिय के हुन्छ ? अहिले यस सम्बन्धमा सरोकारवालसँगको सहकार्यमा सरकारले अनलाइन कक्षा सञ्चालन गरिरहेको छ । ५७ हजारभन्दा बढी विद्यार्थी आजको दिनमा इन्टरनेटको माध्यमबाट पढाउन सकेको छ । अब हामी सबै क्षेत्रमा इन्टरनेटको माध्यमबाट कामलाई अगाडि बढाउँदै छौं । सरकारले विकास निर्माण तथा राष्ट्रिय गौरवका आयोजनाको अनुगमन पनि इन्टरनेटकै माध्यमबाट गरिरहेको छ ।

अन्त्यमा, इन्टरनेट दिवसका अवसरमा सबैले यसको उच्चतम सदुपयोग गर्दै यसबाट विकास निर्माणको काममा सहजता ल्याउन सकोस्, सबैमा शुभकामना गर्दछु ।

२९ माघ, २०८१

Pranav
केपी शर्मा ओली



नेपाल सरकार

सञ्चार तथा सूचना प्रविधि मन्त्रालय

मा. पृथ्वीसुब्बा गुरुङ्ग
सञ्चार तथा सूचना प्रविधि मन्त्री

सिंहदरबार, काठमाडौं
नेपाल

शुभकामना

विश्वव्यापी रूपमा हरेक वर्ष फेब्रुअरी महिनाको दोस्रो मंगलबार मनाइने सुरक्षित इन्टरनेट दिवस यस वर्ष "सुरक्षित इन्टरनेट, सधैंका लागि, सबैका लागि" भन्ने नाराका साथ नेपालमा मनाउन सम्पूर्ण सञ्चार तथा सूचना प्रविधिसंग सम्बन्धित सरोकारवाला निकायहरू तथा आम उपभोक्ताहरूमा सुरक्षित इन्टरनेट २०२५ को शुभकामना व्यक्त गर्न चाहन्छु ।

सूचना तथा सञ्चार प्रविधिको द्रुततर विकाससँगै यसको प्रयोगले विद्य एक गाउँको रूपमा रूपान्तरण गर्न इन्टरनेट प्रविधिले अग्रणी भूमिका निर्वाह गर्दै आएको अवस्थामा यसको समुचित प्रयोगले सबै उमेर समूहका व्यक्तिहरूको दैनिक कृयाकलाप सहज हुने मात्र होइन, देशको समग्र आर्थिक, सामाजिक र साँस्कृतिक विकासमा समेत प्रत्यक्ष सहयोग पुर्याउछ। प्रविधिको गतिसँगै आएका चुनौती तथा जोखिमहरूलाई संगसँगै सम्बोधन गर्नुपर्ने आजको आवश्यकता भएको छ।

अधिकांश जनसंख्या इन्टरनेट सेवामा जोडिँदै आएको अवस्थामा साइबर अपराधका घटनाहरू न्यूनीकरण गर्न आम नागरिकलाई इन्टरनेट प्रविधिमा आधारित सेवाहरूमा सुरक्षाको प्रत्याभूति गराउन पहलकदमी लिनु आजको आवश्यकता हो। यसका साथै ज्ञानमा आधारित समाज निर्माण गर्न इन्टरनेट प्रविधिको पूर्वाधार विस्तार, पहुँच बृद्धि र अनलाइन सुरक्षा साक्षरताका कार्यक्रमहरूलाई व्यापक बनाउन आवश्यक छ। विशेष गरी बालबालिकाको सुरक्षा, व्यक्तिगत गोपनीयता, डिजिटल साक्षरता, र साइबर अपराधको बृद्धि जस्ता विषयहरूलाई गम्भीरतापूर्वक सम्बोधन गर्न यस मन्त्रालयले सुरक्षित, मर्यादित र जिम्मेवार इन्टरनेट प्रयोगलाई प्रवर्द्धन गर्दै आइरहेको छ। यसका लागि केही नीतिगत व्यवस्था भैसकेका छन् भने केही हुने क्रममा छन्। निजी क्षेत्र तथा सरोकारवाला निकायहरूसँग सहकार्य गरी यस क्षेत्रलाई अझ बढी व्यवस्थित र सुरक्षित बनाउन सञ्चार तथा सूचना प्रविधि मन्त्रालय प्रयत्नशील छ।

अन्तमा, "अनलाईन सुरक्षा हामी सबैको अपेक्षा" बोध गरी इन्टरनेट प्रविधिमा आधारित सेवा उपभोग गर्ने सम्पूर्ण सूचना तथा सञ्चार प्रविधि मैत्री सरोकारवालाहरूलाई अनलाइनमा उपलब्ध भएका तथा हुने सेवाहरूलाई सुरक्षित र मर्यादित बनाउन आह्वान गर्दछु। यस सुरक्षित इन्टरनेट दिवसले सम्पूर्ण इन्टरनेट उपभोक्ताहरूलाई अनलाइन सुरक्षा प्रति सजग बनाउन सफल होस् शुभकामना व्यक्त गर्दछु।

मिति: २०८१ माघ २८ गते

पृथ्वी सुब्बा गुरुङ्ग
मन्त्री, सञ्चार तथा सूचना प्रविधि मन्त्रालय

फोन नं. : ९७७-४२११२२२, ४२११६४०, ४२११७०१ (कार्यालय), फ्याक्स नं. : ९७७-१-४२११६००

वेब साइट: www.mocit.gov.np



नेपाल दूरसञ्चार प्राधिकरण

(अध्यक्षको सचिवालय)

शुभकामना

इन्टरनेटको सुरक्षित तथा सकारात्मक प्रयोगलाई प्रमर्दन गर्न हरेक वर्ष विध्वन्यापी रूपमा फेब्रुअरी महिनाको दोस्रो मंगलवार सुरक्षित इन्टरनेट दिवस मनाउँदै आइरहेकोमा "सुरक्षित इन्टरनेट, सबैका लागि, सबैका लागि" भन्ने नाराका साथ आज सुरक्षित इन्टरनेट दिवस मनाउने र वर्षभरी नै विभिन्न कार्यक्रमहरू आयोजना गर्दै इन्टरनेटको सुरक्षित प्रयोगलाई अभियानको रूपमा अगाडी बढाउने सम्पूर्ण दूरसञ्चार सेवाप्रदायकहरू, साइबर सुरक्षाकर्मीहरू, नागरिक समाज, अभियानकर्ताहरू तथा आम इन्टरनेट उपभोक्ताहरूमा सुरक्षित इन्टरनेट दिवस, २०२५ को अवसरमा हार्दिक शुभकामना व्यक्त गर्दछु।

इन्टरनेट प्रविधिको विकास तथा विस्तारबाट आम उपभोक्ताहरूको दैनिक क्रियाकलापहरू सहज र सरल हुँदै आएको छ । ब्रोडब्याण्ड इन्टरनेट सेवाको पहुँच विस्तारबाट आम नागरिकलाई प्रदान गरिने सार्वजनिक सेवाहरू इन्टरनेट प्रविधिमा आधारित हुँदै आउनु सुखद पक्ष हो । इन्टरनेट प्रविधिको प्रयोग बढ्दै जाँदा डिजिटल साक्षरताको कमीले गर्दा र ए. आई. जस्ता नविनतम प्रविधिहरूको आगमनले अवसरको साथै सुरक्षा जोखिम तथा थप चुनौतीहरू पनि निम्त्याएको छ ।

अनलाईनमा बालबालिकाहरू बढी दुर्व्यवहार र हिंसाको शिकार भैरहेको विषयलाई मध्यनजर गरी नेपाल दूरसञ्चार प्राधिकरणले अनलाइन बाल सुरक्षा निर्देशिका, २०७६ तर्जुमा गरेको छ । यसै गरी अनपेक्षित रूपमा साइबर अपराधका घटनाहरू दिनानुदिन बढ्दै दूरसञ्चार सेवा प्रदायकहरू समेत विभिन्न समयमा प्रभावित हुँदै आएको परिप्रेक्ष्यमा दूरसञ्चार सेवालार्इ थप सुरक्षित र विध्वंसनिय बनाउने उद्देश्यले नेपाल दूरसञ्चार प्राधिकरणबाट साइबर सुरक्षा विनियमावली, २०७७ लागू गरी कार्यान्वयनमा ल्याइएको अवस्था छ । साथै इन्टरनेट प्रविधिमा आधारित सेवाहरू प्राप्त गर्ने आम उपभोक्ताहरूको सचेतनाको लागि साइबर सुरक्षासंग सम्बन्धित विभिन्न विषयहरूमा साप्ताहिक रूपमा जनहितमा जारी गरिएको सन्देशहरूलाई एकत्रित गरी सार्वजनिक गरिएको छ । प्राधिकरणबाट विभिन्न प्रदेशहरूमा साइबर सुरक्षासंग सम्बन्धित विषयमा नीति निर्माणकर्ताहरू, अनुसन्धान तथा अभियोजनकर्ताहरू, पत्रकारहरू, विद्यार्थी तथा शिक्षक वर्गहरूसंग नीति संवाद, अन्तरक्रिया, गोष्ठी, तालिम लगायतका कार्यक्रमहरू गरिएको छ । यति मात्र नभई प्राधिकरणले इन्टरनेटका आम उपभोक्ताहरूले सजिलोसंग बुझ्ने गरी सरल भाषामा भिडियो सन्देशहरू समेत इन्टरनेट, रेडियो तथा टेलिभिजनबाट प्रवाह गर्दै आइरहेको छ ।

अन्तमा: यस सुरक्षित इन्टरनेट दिवस, २०२५ को अवसरमा नेपाल सरकारबाट समयानुकूल नीति निर्माण हुँदै जानेछ, सम्पूर्ण दूरसञ्चार सेवा प्रदायकहरूले थप सुरक्षाका उपायहरू अपनाउँदै सेवा प्रदान गर्दै जानेछन् र आम दूरसञ्चार उपभोक्ताहरूले सचेतनाका साथ जिम्मेवारपूर्वक इन्टरनेट सेवा उपभोग, हुनेछ भनी आशा व्यक्त गर्दछु । धन्यवाद ।


भूपेन्द्र भण्डारी

अध्यक्ष



नेपाल सरकार सञ्चार तथा सूचना प्रविधि मन्त्रालय

प.सं.
च.नं.

शुभकामना

सिंहदरवार, काठमाडौं

हरेक वर्ष फेब्रुअरी महिनाको दोस्रो मंगलवारलाई सुरक्षित इन्टरनेट दिवसका रूपमा विश्वव्यापी रूपमा मनाइरहेको सन्दर्भमा यस वर्ष "सुरक्षित इन्टरनेट; सधैंका लागि, सबैका लागि" भन्ने नाराका साथ नेपालमा सुरक्षित इन्टरनेट दिवस २०२५ मनाउन लागिएको छ। यस अवसरमा सूचना प्रविधि तथा सञ्चार क्षेत्रसंग सम्बन्धित नीति निर्माता, नेतृत्वकर्ता, व्यक्ति, संघसंस्था, सरोकारवाला निकाय तथा आम उपभोक्तामा हार्दिक शुभकामना व्यक्त गर्दछु।

विश्वमार्गै द्रुततर गतिमा विकास भैरहेको सञ्चार तथा सूचना प्रविधिको प्रयोग नेपालमा पनि तीव्रतर हुदै गएको छ। आम नागरिकको दैनिक जीवनसंग जोडिएका सेवाहरू अनलाइनमा आबद्ध भइ इन्टरनेट दैनिक कृयाकलापको अभिन्न अंग हुन पुगेको छ। अत्यावश्यक सेवाको रूपमा रहेको यस इन्टरनेट सेबाले राष्ट्रको समग्र आर्थिक, सामाजिक र सांस्कृतिक विकासमा प्रत्यक्ष योगदान पुऱ्याउँदै आएको छ। इन्टरनेट प्रविधिले सिर्जना गरेको प्लेटफर्मले सूचनामा सहज पहुँच पुऱ्याउनुको साथै विश्वलाई एउटै गाँउ जस्तो बनाएको छ। हालका दिनहरूमा यसको दुरुपयोग हुन पुगी केही अपराधिक गतिविधिहरूमा पनि वृद्धि भएको तथ्याङ्कले देखाएको छ। अनलाइनको माध्यमबाट हुने हिंसा, दुर्व्यवहार र साइबर अपराध जस्ता गतिविधिहरूले निम्त्याएको चुनौती तथा जोखिमहरूलाई न्यूनीकरण गर्न आवश्यक पहलकदमी आजको आवश्यकता भएको छ।

साइबर अपराधका घटना न्यूनीकरण गर्न आम नागरिकलाई इन्टरनेट प्रविधिमा आधारित सेवाहरूमा सुरक्षाको प्रत्याभूति गराउन सञ्चार तथा सूचना प्रविधि मन्त्रालय प्रतिबद्ध छ। व्यक्तिगत गोपनीयताको सुरक्षा, डिजिटल साक्षरतामा बढोत्तरी र साइबर अपराधको न्यूनीकरण जस्ता विषयहरूलाई गम्भीरतापूर्वक सम्बोधन गर्न अन्य सरकारी निकाय, निजीक्षेत्र तथा सरोकारवाला निकायहरूसँग सहकार्य गरी यस क्षेत्रलाई अझ बढी व्यवस्थित र सुरक्षित बनाउन मन्त्रालय प्रयत्नशील रहेको विश्वास दिलाउन चाहन्छु। आजको यस महत्वपूर्ण अवसरमा सम्पूर्ण सूचना तथा सञ्चार प्रविधि क्षेत्रसंग सम्बद्ध सबै सरोकारवालाहरूलाई अनलाइन सेवा अझै बढी सुरक्षित र मर्यादित बनाउन आ-आफ्नो क्षेत्रबाट सहयोग गर्न आव्हान गर्दै यस सुरक्षित इन्टरनेट दिवसले आम उपभोक्तालाई अनलाइन सुरक्षा सम्बन्धी विषयमा सचेत बनाउने अपेक्षा सहित हार्दिक शुभकामना व्यक्त गर्दछु।

मिति: २०८१ माघ २८ गते

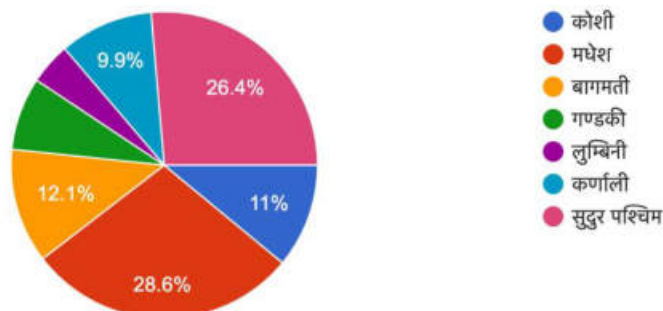
राधिका अर्याल
सचिव

सञ्चार तथा सूचना प्रविधि मन्त्रालय

Appendix C: Children Responses and feedback

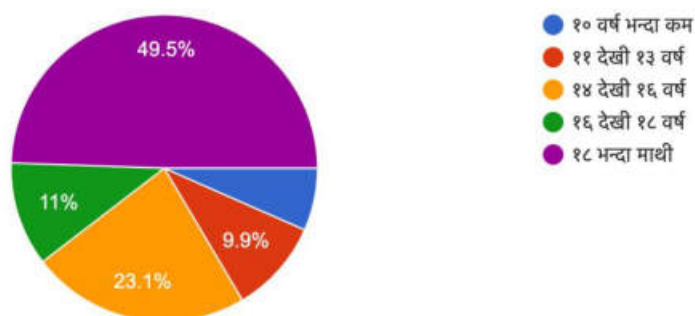
तपाईं कुन प्रदेशबाट हुनुहुन्छ ?

91 responses



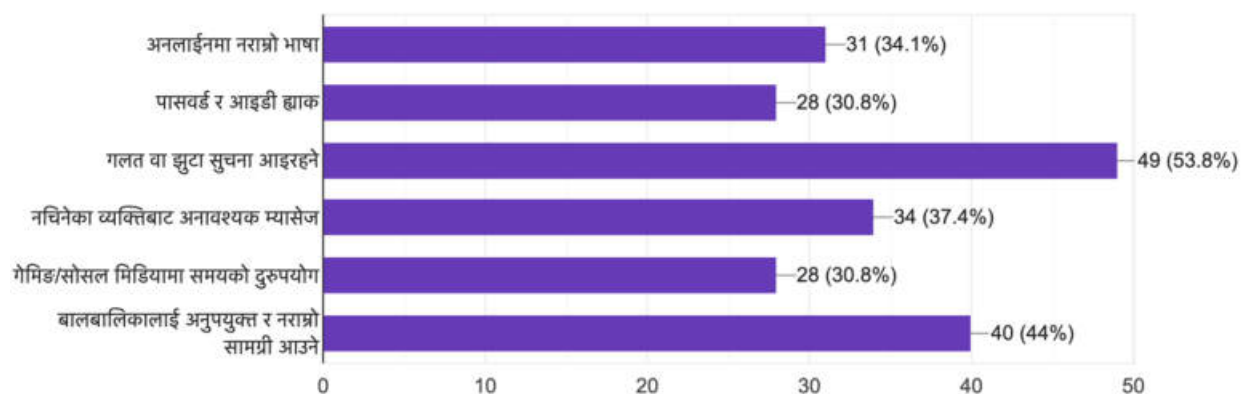
तपाईं कुन उमेर समुहमा पर्नुहुन्छ?

91 responses



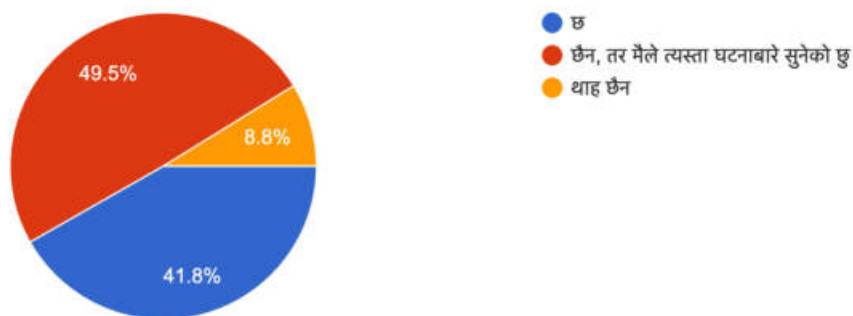
१. तपाईं इन्टरनेट प्रयोग गर्दा ठूलो समस्या के के महसुस गर्नुहुन्छ? (एकभन्दा धेरै छान्न सक्नुहुन्छ)

91 responses



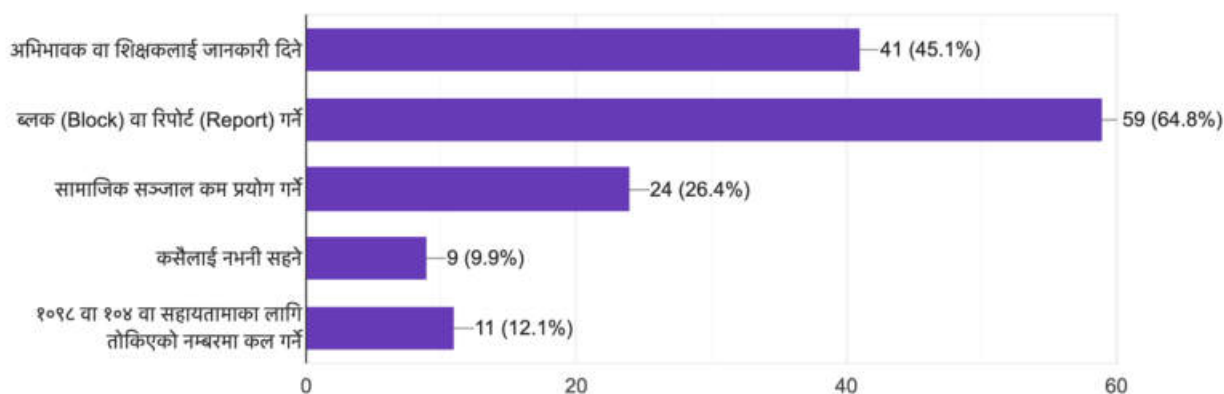
२. इन्टरनेटमा तपाईंलाई कहिल्यै कसैले सताएको वा अनावश्यक सन्देश पठाएको छ?

91 responses



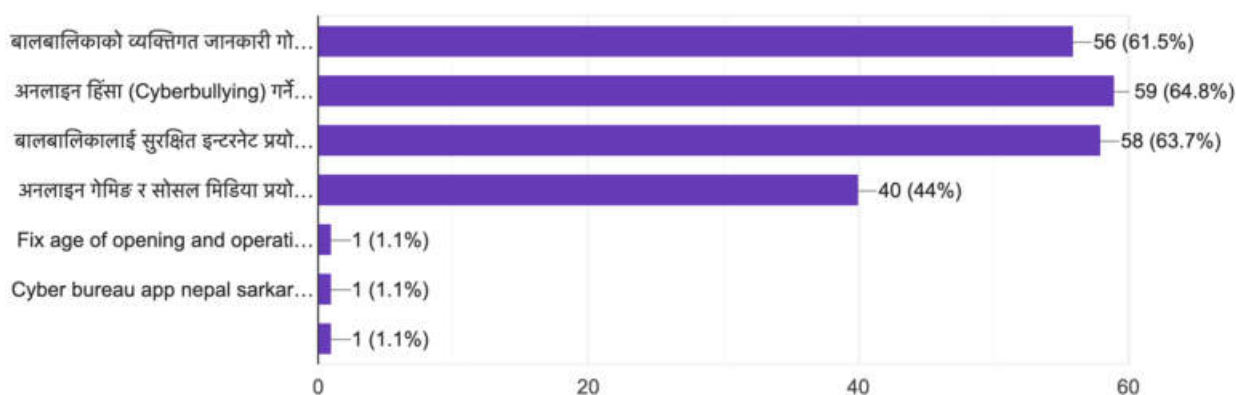
३. अनलाइन हिंसा वा साइबरबुलिङबाट जोगिन तपाईंले के गर्ने गर्नुभएको छ ? (एकभन्दा धेरै छान्न सक्नुहुन्छ)

91 responses



४. तपाईंको विचारमा, साइबर सुरक्षासम्बन्धी नयाँ कानूनमा के के विषयहरू अनिवार्य रूपमा समावेश हुनुपर्छ? (एकभन्दा धेरै छान्न सक्नुहुन्छ)

91 responses



५. तपाईंको विचारमा यदि इन्टरनेट प्रयोग गर्दा समस्या परेमा, सहायता माग्न कस्तो व्यवस्था हुनुपर्छ? (एकभन्दा धेरै छान्न सक्नुहुन्छ)

91 responses

