Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 2 Article 5

October 2023

Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal

Raj Kumar Dhungana
Kathmandu University, School of Education, rajkumar@kusoed.edu.np

Lina Gurung Dr
Kathmandu University, lina@kusoed.edu.np

Hem Poudyal
University of Bremen, Germany, poudyalhem@gmail.com

Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal

Abstract

Increased exposure to technologies has lately emerged as one of the everyday realities of digital natives, especially K-12 students, and teachers, the digital immigrants. Protection from cybersecurity risks in digital learning spaces is a human right, but students are increasingly exposed to high-risk cyberspace without time to cope with cybersecurity risks. This study, using a survey (N-891 students and 157 teachers) and in-depth interviews (27 students and 14 teachers), described the students' cybersecurity-related experiences and challenges in Nepal. This study revealed that the school's cybersecurity support system is poor and teachers has very low awareness and competencies to protect students from cybersecurity-related challenges. To create a safe cyberspace for learners, it is urgent to enhance the cybersecurity awareness and skills of teachers, as the existing infrastructure is weak and there is a significant gap related to the cybersecurity awareness between students and teachers. Poor cybersecurity is one of the significant barriers to the quality of education in Nepal. In the age of information and technology, effective collaboration among parents, teachers, and students, the multi-generational learners, is the prerequisite for ensuring children's rights to learn in all settings including cyberspace.

Keywords

Cybersecurity, child right, digital learning, multi-generational learners

Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal

Raj Kumar Dhungana, PhD
Visiting Faculty
Kathmandu University School of Education
Nepal
ORCID: 0000-0003-4894-4230

Lina Gurung, PhD
Assistant Professor
Kathmandu University School of Education
Nepal
ORCID: 0000-0003-4268-2575

Hem Poudyal
University of Bremen
Germany
ORCID: 0009-0007-7534-3808

***Abstract*—Increased exposure to technologies has lately emerged as one of the everyday realities of digital natives, especially K-12 students, and teachers, the digital immigrants. Protection from cybersecurity risks in digital learning spaces is a human right, but students are increasingly exposed to high-risk cyberspace without time to cope with cybersecurity risks. This study, using a survey (N-891 students and 157 teachers) and in-depth interviews (27 students and 14 teachers), described the students' cybersecurity-related experiences and challenges in Nepal. This study revealed that the school's cybersecurity support system is poor and teachers has very low awareness and competencies to protect students from cybersecurity-related challenges. To create a safe cyberspace for learners, it is urgent to enhance the cybersecurity awareness and skills of teachers, as the existing infrastructure is weak and there is a significant gap related to the cybersecurity awareness between students and teachers. Poor cybersecurity is one of the significant barriers to the quality of education in Nepal. In the age of information and technology, effective collaboration among parents, teachers, and students, the multi-generational learners, is the prerequisite for ensuring children's rights to learn in all settings including cyberspace.**

Keywords— cybersecurity, human rights, digital learning, multi-generational learners

I. Introduction

With increased digitalization, access to the internet, a safe learning environment, and digital literacy are being recognized as basic human needs and rights. In 2016, the UN General Assembly passed a non-binding resolution declaring internet access a human right. Article 9 of Nepal's Constitution, under the fundamental rights, has ensured Nepali citizens' rights to communication. It mentioned, "No radio, television, online, or other forms of digital or electronic equipment will be closed or seized". Article 28 ensures an individual's right to privacy, including data, documents, correspondence, and matters relating to his or her character (Secretariate, 2015). Children has the rights to learn in a safe environment in all settings including cyberspace (Florek & Eroglu, 2019).

Safe cyberspace is important for all so that they can exercise their fundamental rights to communication while maintaining their rights to privacy. Access to broadband internet has grown in Nepal from 9% in 2011 to 37.7% in 2019 (GoN, 2019). Similarly, internet access has reached 90.56 percent of Nepal's population, including mobile internet users (NTA, 2021). With increasing access to ICT, Nepal is also making efforts to make cyberspace safe, and it progressed to 94th position in the Global Cybersecurity Index 2020 from 106th in 2018 (ITU, 2020).

This is the digitalization era, also known as the era of the netizen community, where technology is seen as a process of social interaction and has been increasing (Achmad, 2021). The use of digital means has expanded in the education sector. In Nepal, out of over 35 thousand schools, 47.2% have access to the internet (NTA, 2021). Further, a World Bank study suggests that 58 percent of households have access to the internet, including mobile phones (Radhakrishnan et al., 2021). There are limited studies on how the digital native students are getting support from the teachers, who are the digital immigrants.

The rapid change in ICT is causing students and teachers to have significant generational differences in terms of digital exposure. Most of the teachers are digital 'immigrants' (Prensky, 2001), and they are teaching the 'digital natives' students (Lisenbee, 2016). The 'native' students are exposed to enormous technologies without time to be prepared and cope with the possible risks and possible negative consequences. The 'immigrant' teachers' digital literacy has increased significantly over the last two decades, yet they are not yet fully ready to support the 'natives' students in creating safe cyberspace. For example, 41% of English language teachers have learned to use ICT in their formal education or training in Nepal, while most of them have access to smartphones and/or computers with internet facilities (Saud, 2021).

While the use of internet in education is increasing, , It is essential to make digital learning safe for all to minimize cybersecurity risks such as cyberattacks, phishing, and cyberbullying. In general, there are high risks of compromising the safety and security of individuals in cyberspace, but people are largely unaware of these risks (Kortjan & Solms, 2014). Hence, it is strenuous to understand cybersecurity awareness of teachers and students to protect children's rights to safety from unknown individuals, with fake identities living in the unknown zone.

At large, cybersecurity awareness is quite shallow in Nepal (Acharya & Dahal, 2021). Schools are facing tremendous challenges in making cyberspace safe for children

and teachers. Students without cybersecurity awareness are at higher risks while using ICT in school and at home. They need to learn nitezenship education comprising ethics, media and information literacy, participation, and critical resistance (Choi, 2016). Teachers are often clueless about students' digital behavior and the possible risks. Along with increased access to ICT, cybersecurity risks such as cyberattacks, and cyberbullying have increased in Nepal (Dhungana, 2014). A study carried out in Nigeria revealed that students are facing various cyber-risks, such as cyberbullying and provocative content, followed by sexual solicitation (Adeola &Abiodun, 2021).

Cybersecurity comprises the protection of critical information infrastructure, as well as elements that are considered critical information infrastructures, such as information networks of small and medium-sized enterprises, or personal computers (Moise, 2016). Cybersecurity is about a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, organization, and users' assets (ITU, 2008).

Considering the fact that individual right to privacy is a fundamental human right (article 12, Universal Declaration of Human Rights) and cybersecurity is an essential aspect to ensure individual's privacy in the digital world), this paper used a human rights-based approach as the theoretical framework. Children have the right to be protected from all forms of violence and threats in all circumstances, and the parents, school, and state have the responsibility to ensure their rights. Nepal, as a party to the Convention of the Rights of the Child (CRC) and Agenda 2030, has the responsibility to provide children with an effective and safe learning environment. The learning environment in the digital era comprises a safe environment in the changing cyber and physical spaces (United Nations (UN), 1989). Nepal's Comprehensive School Safety Implementation Guideline 2019 has identified various risks in schools (Ministry of Education, Science, and Technology, 2019), but the cybersecurity risk has not been recognized as one of the safety concerns. Internet access has a significant impact on human rights, and it is human rights and fundamental freedoms are relevant and applied online and offline (Kothari, 2019). The state has the duty to provide a safe environment for learning, including ensuring cybersecurity for all, but especially for the children who, compared with adults, are unable to identify cybersecurity-related risks until it is too late and can easily fall victim to online abuse (Quayyum et.al., 2021). At school, the teachers have the duty to protect children from cybersecurity risks so that there is enabling learning environment for all children.

The purpose of this paper is to understand teachers' and students' awareness of cybersecurity risks in Nepal. This paper contributes the growing debate of cybersecurity in education in the low and middle-income countries that recently invested a large amount of resources in establishing ICT system and the options for online learning but they are facing challenges to create safe digital space for their children and teachers.

The findings and conclusions of this study cannot be generalized because the study sampling was not statistically randomized and representative.

The situation in Nepal was very different 10 years ago as access to the internet until 2011 was only 3% (CBS, 2011). Currently, most teachers and students have internet access, and they are part of a netizen society (Achmad, 2021). With the expansion of digital technology and access to the internet, children are spending more time on online platforms. In general, Mohr and Mohr (2017) revealed that teachers are unable to follow the pace of technologies, and consequently, they cannot support students to address cybersecurity issues such as internet safety, cyberbullying, identity theft, online phishing, privacy, passwords, securing private information, and internet strangers (Yuliana, 2022). Further, teachers are not empowered to use o collaborative teaching pedagogy following a constructivist learning approach, while collaborative pedagogy is effective for developing unplugged computer science activities (Fees et al., 2018). Phyak et al. (2019) revealed that 64% of teachers in Nepal do not use ICT in school due to a lack of training, and furthermore, they do not have access to digital tools in school. It shows that the teachers who are mostly the 'digital immigrants' will be irrelevant when 91% of the country's population has access to internet service (NTA, 2021). In addition, there are limited or no collaborative teaching practices in Nepal, as the majority of the old generation teachers have limited ICT knowledge and skills (Rana & Rana, 2020).

Based on exposure to digital awareness and digital generation, the teachers and students are defined as digital 'immigrants' and 'natives' respectively. Digital immigrants and natives have unique attitudes, behaviors, expectations, and motivational buttons (Leite-Trambly & Obasi, 2018). E-learning is based on the social categorization of generations, which produces a different inter-generational learning environment (Yawson & Yamoah, 2020). For example, the 'natives' had access to the internet from their childhood, while the 'immigrants' started using computers in their late adolescent period. Immigrants and students have the right to be digitally literate, to be protected from cybercrimes, and cyberattacks, and to exercise their rights to teach and learn in a safe space. Giri and Shakya (2021) identified some of the new cybercrimes, such as ransomware, spear phishing, privacy leaks, harassment, child pornography, and the dissemination of mendacious information. Teenagers, particularly students, are likely to be the most common victims of cyberbullying. Even teachers can be the victims of bullying for example, through a simple mean statement posted against them on the wall of social networking (Rajbhandari & Rana, 2022). Most school-going adolescents experience cybersecurity issues such as cyberbullying in school (Dhungana, 2018). Similarly, the state has the duty to protect human rights in cyberspace (Rona & Aarons, 2015). Hence, it is important to understand the duty-bearer state's policy measures to protect students from cybersecurity issues.

A. Evolving Cybersecurity Policies in Nepal

Cybersecurity policies are belatedly evolving in Nepal. One of the first ICT in education policies, the ICT in Education Master Plan 2013–2017, presented ICT as an innovative and effective means of teaching and learning and a means to expand access to education. In line with this plan, the government of Nepal and the private sector have been investing large amounts of resources in expanding the internet and technologies in school (Dhungana, 2014). For example, the Government's Information and Technology Framework 2019 presents Nepal's vision to achieve good governance, development, and prosperity through digital Nepal. It

emphasizes the wide use of information technologies and identifies education as one of the eight drivers to promote digital Nepal envisioned promoting smart classrooms, online learning, a laptop-in-rent program, an education information system, a centralized school admission system, biometric attendance, CCTV cameras, and mobile learning. Similarly, to address pertinent issues of the digital divide and cybersecurity, this strategy included a strategy to mitigate the digital divide and establish a national cybersecurity center (GoN, 2019). However, similar investment has not been prioritized in making cyberspace safe while cyberattacks, hacks, and security breaches are daily happenings (Arora et al., 2006; de Bruijn & Janssen, 2017).

In line with the Convention on the Rights of the Child and its Optional Protocol on the Sale of Children, Child Prostitution, and Pornography (UN, 1898), there is a need to protect children from such abuse and exploitation. The Nepal Tele-Communication Authority (NTA) has issued the Online Child Safety Guidelines 2019 to reduce the increasing incidence of child abuse through online media through joint initiatives of stakeholders and for the safe use of the internet (NTA, 2019). The guideline contains detailed provisions on what online service providers, including NTA, should do for children, households, and communities, information on websites and apps used by children, safe use of the internet on school computers, and the role of stakeholders. Besides that, the guideline is targeted at parents, guardians, and educators.

In addition, the government formulated a cybersecurity by-law to implement cybersecurity standards to protect ICT infrastructure and information systems of internet service providers from various malicious attacks and threats and build the trust and confidence of users towards using ICT technology and services (NTC, 2021). These guidelines are geared toward helping adults manage the risks of the internet and connectivity but do not include a strategy to build awareness among critical stakeholders like teachers and students.

The Ministry of Women, Children, and Senior Citizens approved an Online Child Protection Procedure 2021 in line with the existing Children's Act to curb online abuses of minors (GoN, 2021). This procedure requires schools to use encrypted computers for internet connectivity, monitor children's online activities, and install software that helps filter harmful content and limits their access to such content on their devices. Similarly, schools must provide designated teaching materials for children. The procedure calls for each educational institution to establish a grievance handling system to address complaints related to online child abuse that may happen in school and designate a focal person to deal with such complaints. The schools have also been restricted from collecting and uploading photographs and personal details of children. Any school wishing to put up photographs and personal details of children shall obtain the prior consent of the guardians concerned for that purpose. It requires schools to encourage children to lodge a complaint related to online abuse (GoN, 2021). However, schools lack the necessary ICT infrastructure and competent human resources to follow up on the child protection procedure.

Further, there is very little capacity of the Government to compel social media operators to make the content free of online child abuse and discourage the use of offensive content to protect all users, including children (The Himalayan Times, October 27). The use of ICT in education and online learning has several benefits, but it can be precarious if state is unable to manage cybersecurity concerns in schools and families where children, teachers, and parents, the multicultural learners, are expected to engage in learning processes.

B. Study Purpose

Having access to digital tools and the ability to use digital applications are minimum prerequisites to mitigating the learning gaps among digital immigrants. Nonetheless, only a small percentage of teachers (9.5%) use digital applications such as email, MS Word, MS Excel, and PowerPoint regularly in teaching, while 29.4 percent of teachers have 'never' used such applications for classroom teaching, while only 4.8 percent of teachers consider themselves 'experts' in the use of ICT in education in Nepal (Phyak et al., 2019).

The mainstream research and policy concerned with children's well-being have paid very little attention to the cybersecurity issue (Livingstone & Third, 2017), and there are very limited studies available that present the cybersecurity challenges and awareness of the multi-generational learners in Nepal. To understand the cybersecurity challenges faced by multicultural learners' and their awareness, this paper describes some of the strengths and weaknesses in cybersecurity awareness among students in Nepal. This paper used a human rights-based approach as a theoretical framework, recognizing a safe digital space as one of the enabling conditions for quality learning and it considers cybersecurity as human rights. The major purpose of this study is to understand the cybersecurity challenges faced by multi-generational students and teachers and describe their cybersecurity awareness in the digital learning space. The major research questions of this study are:

- How have the Nepalese students, the 'digital natives', experienced cybersecurity challenges?
- How is the awareness of the teachers, the 'digital immigrants' and the students of creating a safe digital space?

II. METHODOLOGY

This is a mixed-methods study including a purposive sample survey, key informant interviews, a literature review, and comparative analyses. A total of 891 K–12 students and 157 school-level teachers participated in the survey. An online survey conducted among the students and teachers helped to understand how the students and teachers are experiencing cybersecurity issues in school. The students and teachers were purposefully selected to capture the views of multi-generational learners, considering teachers as life-long learners. The survey questionnaire was circulated to the private and public schools that were applying online teaching modes during the COVID-19 restrictions. The survey questionnaire is included in Appendix 1. Of the total 891 students, 45% were girls, and 51% of them were 10–18 years of age. Of the 157, total respondents, 71% are female teachers, 95% are millennials, born before 2000, and 73% are above the age of 30.

In addition, qualitative key informant interviews (KII) were conducted with teachers and students to get in-depth qualitative information. For collecting qualitative information, key informant interview schedules were circulated among the 75 schoolteachers of whom 14 teachers responded through email. Similarly, a total of 27 students participated in the key informant interview.

III. FINDINGS

A. *Access, and Use of ICT in School*

A total of 157 teachers participated in the survey, of whom the majority (71%) were female teachers, and more than half of the teachers were 29–40 years. 97 percent of teachers have private Wi-Fi at home, 37% of them use mobile data and 46 percent use the internet on a shared basis. Most of the teachers (87%) use YouTube, Facebook (84%), and Instagram (46%). Only a few teachers use Snapchat (19%) and blogs (18%).

Students have access to all types of information as they are connected to the internet, which has very limited or no security features. This has both positive and negative impacts. Most of the students responded that their parents have a basic level of ICT awareness, for example, the ability to use smartphones or computers.

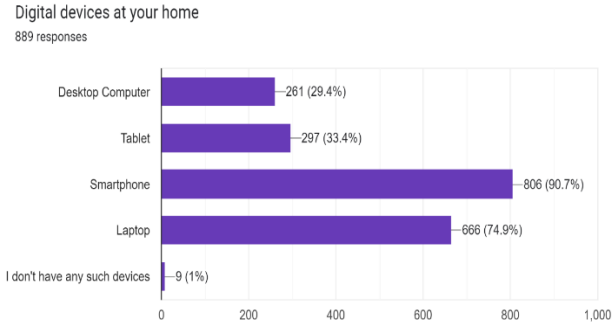

Fig. 1. Digital divices at home

Figure 1 shows that almost 95 percent of parents can use ICT tools, particularly smartphones. This information is consistent with another finding, '90% of students responded that they have smartphones in their homes and 91% have access to Wi-Fi networks'. Most students have access to Wi-Fi and smartphones at home; yet, the students did not use the subsidized data packs provided by key internet service providers like Nepal Telecommunication Corporation (NTC) and NCell.

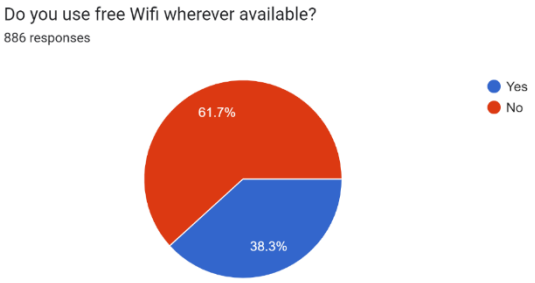

Fig. 2. Use of free Wi-Fi

The majority (78%) of the respondents mentioned that their mother has basic competence in the use of ICT, and the mothers have less than half (15%) of the advanced ICT skills compared to the fathers (33.5%) of the students. Among the 889 respondents, 91 percent have access to smartphones at home, and 74 percent have access to laptops. The 33 percent students have access to tablets, and 29 percent have desktop computers. In addition, 92 percent of students have access to private wifi at home, and 29 percent of them have been using subsidized mobile data provided by the two largest mobile data-providing companies in Nepal: NCELL and NTC. Figure 2 shows that a large percentage (38%) of students use free wifi wherever it is available, but the majority believe that using free wifi could cybersecurity risks.

Forty-two percent of the students responded that they share wifi with other than family members, and 38% of students use free wifi wherever it is available without considering the possible risks. Figure 3 shows that most students have been using YouTube (94%), Facebook (70%), Instagram (62%), Snapchat (39%), Twitter (19%), and blogs (16%). Students are using 49 types of social media, including pirated sites, Discord, Viber, games, Mobile Legend, and Pinterest, among others.

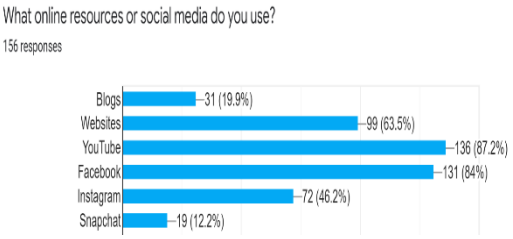

Fig. 3. Social media users-students

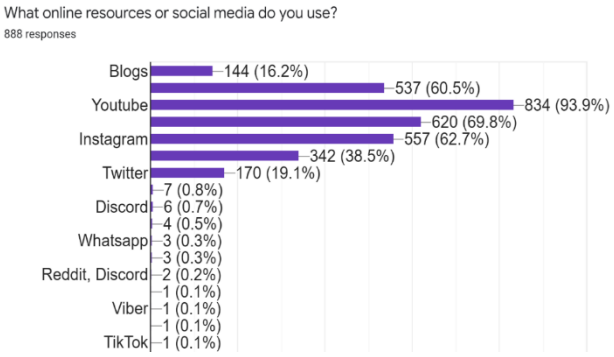

Fig. 4. Social media users - teachers

Figure 4 shows that the teachers are using a lower number of social media than the students and such social media are more conventional types such as blogs, websites, YouTube, Facebook, Instagram, and Snapchat. Since the teachers are using a lower number of digital tools than the students, they are likely to be less aware of the cybersecurity risks that the students might have been facing.

B. *Cybersecurity Awareness among students and teachers*

Students and teachers are the learners engaged in education using various types of ICT tools and the internet. Firstly, this study found a large gap in cybersecurity awareness and skills. The survey results show that 47 percent of respondents are either fully or partly unaware of the risk of using online resources, and 37 percent of them do not feel safe and protected when using online resources. Ninety-five percent of students heard about cybersecurity. Though, 33 percent of respondents use non-genuine or scam websites for downloading or watching movies and other channels. 18 percent of students receive inappropriate messages, such as offensive or humiliating text, images, or videos. Only 16% of

students are informed that they can be the victims of cyberbullying.

Most respondents (53%) are aware of the risks of ICT and online resources, while 47% of students feel that they are partially aware or unaware of the possible cybersecurity risks. In line with their awareness of cybersecurity, 38 percent of students responded that they do not feel safe in online spaces.

Training and formal education enable students and teachers to make cyberspace safe. Fifteen percent of teachers responded that they have not received any training on online teaching, while over half of the total teachers (53%) responded that they have received training on online teaching. Further, 5% students had not heard about cybersecurity, 33 percent actively watched or downloaded movies or series from non-genuine or scam Websites, and 18 percent received inappropriate messages such as offensive or humiliating text, images, or videos. Contrarily, 16 percent of students were unconcerned that they can be the target of cyber-attack.

Teachers have significant roles in cybersecurity in schools as one of the key agents of the state. The overall gap in teachers' knowledge and skills related to cybersecurity is significantly high, as teachers are exposed to a lower number of digital tools than students. Only 67 percent of students can report any inappropriate cyber behavior to their school authority or teachers. In addition, a very limited number (39%) of respondents have discussed inappropriate cyber behaviors and issues with their family members. Half of the respondents received some support and orientation on cybersecurity issues, and 55 percent believe that schools can provide cybersecurity support.

Using a strong password and different passwords for different platforms is one of the prerequisites to cybersecurity. Forty percent of respondents (N-887) shared that they regularly or partly share the passwords of their accounts with their friends and family members and 47 percent of them do not use different passwords for different apps and emails. Similarly, 25 percent of the students respond to strangers' messages, video calls, or friend requests, as they do not consider such activities to be high-risk behavior. Furthermore, 18 percent of respondents are not aware that they should pay careful attention to the privacy settings on their social media sites, such as Facebook, Instagram, WhatsApp, etc.

TABLE I. TEACHERS TRAINED IN CYBERSECURITY.

Trained on cybersecurity	Little orientation received	Not received any training
7.8%	39.8%	53%

Table 1 shows that, on the one hand, only 12 percent of teachers in the survey believed that they were highly confident in safely using ICT, while the majority (67%) of the teachers consider that they only have a basic level of computer operating skills, but don't have knowledge and competencies related to cybersecurity. On the other hand, 34 percent of students, partly or fully, have not received any type of instruction or support from school, parents, child clubs, or others on the safe use of Internet. Similarly, 55 percent of students have received orientation about legal punishments if they do not follow the internet codes of conduct. It is very important to note that more than half (53%) of teachers have not received any form of training related to cybersecurity. Low cybersecurity awareness and skills among teachers are the same in other similar countries in Asia. For example, 60 percent of teachers cannot use ICT in Malaysia (Zulkifli et al., 2020).

The state has yet to fulfill its duty to train teachers so that they can create a safe space in the digital learning environment. The survey shows that 45 percent of the teachers are either not oriented or partly oriented on Internet codes of conduct. More importantly, teachers do not practice safe behavior. For example, 24 percent of them mentioned that they installed an antivirus program on their computer, and 47% of teachers responded that they were unable to deal with the cybersecurity challenges. In addition, 23 percent of teachers are not aware that some students send or receive offensive messages, and rumors are spread and humiliated through social media.

Furthermore, only 58 percent of teachers use different passwords across different websites and accounts; 47 percent of teachers scan for viruses before downloading any files; and 58% update anti-virus programs regularly. 23 percent of teachers share their passwords with others; 42 percent of students use the same password for their multiple accounts; 15 percent of participants respond to a stranger's message, friend request, or chat and 23 percent do not scan any files before such files are downloaded. Teachers' poor cybersecurity behavior also affects their ability to support students' safe internet usage. Figure 5 shows that more than 34 percent of students are fully or partly unable to report to their teachers or school authorities any type of inappropriate cyber behavior in their school.

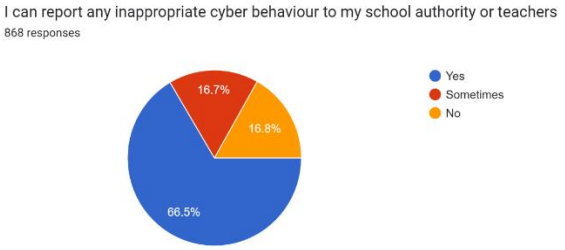

Fig. 5. Students' ability to report cybersecurity issues

Sixty-one percent of teachers in the survey understood Internet codes of conduct and followed them, while the remaining 39 percent mentioned that they were unfamiliar of such codes of conduct. The school authority has been providing instruction to the teachers. Fifty-nine percent of the total teachers mentioned that they received instruction from the school to follow appropriate internet behavior. Yet only 33.6 percent of them received proper orientation about the legal consequences of not following Internet codes of conduct. While the prevalence of cybersecurity issues is quite high, 28 percent of teachers have never discussed issues related to internet safety with school authorities, and 79 percent of them have never discussed such issues with police or other experts. Only 31 percent of teachers are aware of the cybersecurity policies, and 33 percent are aware of the cybersecurity support institutions.

There are some good examples, as shared by the teachers. One of the teachers shared a positive case, "Schools have been providing cybersecurity classes. It is in the national curriculum as well. In the schools I have worked with, we call police officers and child rights activists to talk about these issues. Parent awareness sessions have also been helpful".

Similarly, in some schools, teachers have been trained in cybersecurity and are taking active steps to be aware and guide students in their classes. The onus of cybersecurity is not only on the 'computer teacher' but on each member of the school community and it is human rights.

Some teachers responded that students mostly report cases of password hacking, invasion of privacy, and cyberbullying. However, there is no formal system to register such complaints, and there is no systematic system to support their students. Other teachers said that the students were addicted to digital games and videos, Tik Tok, and Facebook, which resulted in poor reading and writing skills among them. In addition to cyberattacks, multi-generational learners are experiencing cyberbullying.

C. Cyberbullying as a Major Cybersecurity Issue in School

Over 54 percent of students responded that they have experienced cyberbullying regularly or for some time and that it has affected their education, and about 40 percent of students believe that such bullying has been affecting their self-esteem and public image and that they are feeling rejected in their group, and thus having negative consequences for their education. The highest percentage of the students (19%) responded that cyberbullying is a major cybersecurity issue. Of the total, 4 percent of students experienced a serious form of cyberbullying, and 11% of students have received sexually inappropriate messages like nude or nearly nude photos. One of the students responded that,

I think so-called "zoom bombers" who disturb the class with disturbing acts and videos might be mental harassment for students as well as teachers. So, from my point of view, if that could be stopped, then it would be much better.

This survey revealed that a total of 10 percent of respondents have been experiencing cyberbullying via SMS, chat, and other community sites, receiving nude videos or photographs. Similarly, 11 percent of students' online accounts were hacked, and 9.3% of students reported that their account was blocked by hackers. As a result of these cybersecurity issues, 14 percent of students attending this survey shared that they experienced negative feelings and emotions—embarrassment, unhappiness or sadness, loneliness, powerlessness, depression, and anxiety. Similarly, 28.4 percent of respondents partially experience negative feelings and emotions. Cyberbullying causes problems with behavioral attitudes, social norms, perceived behavioral controls, social media use, a lack of parental controls, and a lack of regulations (Alotaibi, 2019).

Cybersecurity risks are not different based on students' exposure to each of the cyber-risk types based on their age groups (Adeola & Abiodun, 2021). Teachers are also experiencing various cybersecurity issues, for example, cyber addiction or dependency. Reed, (2016) revealed a positive correlation between cyberbullying and the students' depressive symptoms.

D. Cybersecurity Support to the Students

The students and teachers were asked what support systems they have been receiving from their school. In response, only 60 percent of students responded that they receive some sort of cybersecurity support from their school. The students responded that 72 percent of teachers can help them if they encounter a minor cybersecurity issue. It is positive that most of the students trust the teacher's digital competencies. The digital competencies of parents are relatively lower, as 38% of students believe that their parents are unable to help them to address cybersecurity issues. Almost 40 percent of the students responded that they don't get cybersecurity support at home or school. Therefore, in the absence of collaborative teaching practices in school, those students either try to address such challenges by themselves or become victims of the poor cybersecurity system.

Very few (10%) teachers responded to the issues about 'students hacking teachers' emails and private information and the school's account.' Such cases are mostly unnoticed if the incidences are minor. Nonetheless, in some cases, schools are acting against the students involved in hacking the school's classified information.

The government mechanism to address the cybersecurity system in Nepal is centralized and not friendly for young students. The Cyber Bureau of the Nepal Police looks after the cybercrime-related issues. The bureau is responsible investigating cybercrime, increasing awareness of cybersecurity in cooperation with stakeholders and experts, investigating cyber-attacks, developing human resources to prevent cybercrime, and exchanging information related to cybercrime (Nepal Police, 2022). Though, a large percentage (45%) of students are unaware of any government system that helps them with cybersecurity-related issues.

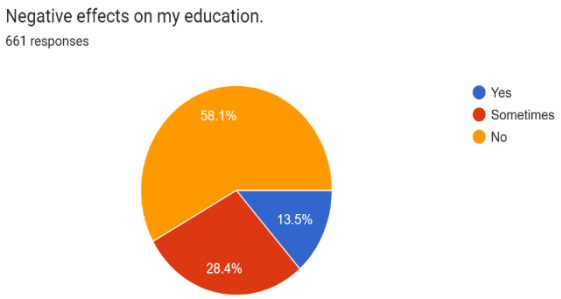

Fig. 6. Negative effects due to cybersecurity issues

Students are willing to learn and participate in cybersecurity-related training. One of the teachers shared that students are interested in cybersecurity training. She said, "The students responded quite well to training and are interested in learning more as this is an issue that affects their home lives too." In general, students are happy that they can use ICT and the Internet for learning. One of the teachers mentioned,

Online learning is somehow safe in Nepal. But like Zoom, Nepal should launch its video meeting app including both Nepali and English. There should be proper facilities so the government can keep track of how many students are enrolled.

The students are more excited that they can use ICT in education. The use of ICT in education is considered a burden to the education system because it demands an increased budget, ICT-friendly teachers, and an effective school management system.

Most of the students wanted to have increased awareness among teachers and all students, including cybersecurity-related education in the formal education system, providing necessary skills and tools to the teachers related to cybersecurity is a highly recommended action. Highlighting the need for regular cybersecurity orientation, one of the respondents said, I wish cybersecurity orientation and

workshops are needed to be conducted by the school or by other resources for the teachers and the entire student body at the school to avoid digital crime or are victimized.

Teachers demanded workshops, including topics such as maintaining confidentiality and victim safety. One of the students who participated in KII mentioned, “Talking about our school, a matter that could be solved privately was blown out and made known to everyone, so I have a distrust of the school regarding my case of cybersecurity. I make a humble request to conduct a program for the teachers and school authorities. This may help solve the problem, as teachers aren't equipped or wise enough to help the matters.”

Students suggested the government enforce laws and regulations and increase awareness among students and teachers on cybersecurity issues. Another student mentioned that "everyone should be given the necessary skill generating education in school to protect themselves from scammers and black-hat hackers so that our passwords will not be hacked without our awareness.”

Further, some students mentioned using trusted online platforms such as Teams and Zoom for conducting online classes. Similarly, the students suggested tightening the rules and regulations, and increasing internet security by the service providers, and making government rules and regulations public. One of the respondents mentioned that cybersecurity issues should be taken seriously by the government and that criminals should get harsh punishment. They also suggested that the service providers invest to ensure security provisions in their system. One of the responses in KII,

Scams should be controlled by the respective ISP of the country so no one could access any kind of website or link program related to cybersecurity. The punishment for being involved in cybercrime should be tough for lower grades so that students and teachers are aware of the punishment for being involved.

Installing monitoring software on school computers is the best way to ensure a safe learning environment during distance learning. Some students suggested that students should be responsible and learn safety measures while using the internet. The government should provide sufficient resources to install anti-virus and other safety systems on computers. The police need to increase their capacity to respond to cyberbullying and crime. Research suggests that students' communication skills and collaboration are the most critical soft skills enabling them to deal with cybersecurity issues (Jones et al., 2018). Participants also suggested that the students provide education related to ethical hacking.

Students suggested establishing a complaint mechanism to address cybersecurity issues in school. Schools need to establish and operationalize a complaint mechanism with high priority to ensure cybersecurity for children. In addition, students suggested making provisions for strong punitive measures for the perpetrators of cyberbullying and cybercrime.

Teacher development in cybersecurity means investment in critical infrastructure (Chowdhury & Gkioulos, 2021) to create school safety and make learning effective. Collaboration between teachers, students, and parents is needed to tackle cybersecurity issues. One of the students suggested that we share the cyberbullying or criminal offenses with parents, teachers, or elders and seek help immediately. Students suggested enforcing the mandatory provision of having a strong password for users. Students and teachers can address most of the cybersecurity risks if they have critical cybersecurity awareness.

Due to the poor cybersecurity system, students and teachers are experiencing bullying, harassment, and distraction, resulting in several negative effects on learning, such as disturbance in education, stress, the suicide as reported in various academic studies (Alotaibi, 2019; Dhungana, 2014; Phyak et al., 2019). Teachers participating in the survey also suggested ways to make digital learning spaces safe. Further, for improving cybersecurity, the participants suggested increasing investment in research related to children's online behavior and risks, and increasing awareness among students and teachers about cybersecurity, cybercrime, and cyberlaw, and implementing the existing regulations. Digital literacy is very poor in the existing education system, as it only focuses on providing computer training and using the Internet for education. Low parental awareness could be another reason for children’s lower cybersecurity awareness levels (Zulkifli et al., 2020), indicates the need of cybersecurity-related lessons in parenting education.

Some of the teachers in school should have advanced skills so that they can handle the difficult issues related to ICT and cybersecurity. One of the teachers suggested, "Local government should mobilize young volunteers in schools to build the cybersecurity competencies of teachers and students because our level of awareness is very low." A total of 43.4% of students are not aware of any cybersecurity government policies. In addition, they suggested making a provision for regular practical orientation to the teachers since the current teacher professional training course does not have cybersecurity modules, while all teachers need at least basic training on online safety and critical infrastructure for the protection of learners (Chowdhury & Gkioulos, 2021), as the existing infrastructure is poor to cope with new cybersecurity challenges.

E. CYBERSECURITY CHALLENGES FOR STUDENTS AND TEACHERS

The findings of this study give some important perspectives on how different generations in economically poor countries like Nepal are coping with cybersecurity challenges. It reveals that conventional child protection actors like teachers and parents have inadequate awareness and skills to protect children and make digital learning safe. Therefore, students need skills to protect themselves, as economically poor countries are unable to invest large numbers of resources to cope with cybersecurity challenges (Solms & Solms, 2015).

Further, the state can't ensure quality education without making cyberspace safe for children and teachers, as digital learning has already been an integral part of education. Though, any single state cannot fully ensure cybersecurity, as it is a global phenomenon. Most high-tech products are created and controlled by high-tech professionals of the private companies companies such as Facebook, Twitter, Google, etc than the government. Regulating internet service providers and large social media sites such as Facebook, Twitter, and Youtube is tough for the least developed countries like Nepal. Moreover, it is most likely that any efforts to control such digital space can be criticized as a state's efforts to 'control media', which is against the principle of human rights.

If trained, teachers and the school can use various ways to help students facing cyber-attacks, for example: considering backup solutions; firewalling security hardening and configuration of the right technology; filtering email and the web, prevention of data leakage; mobile security solutions; restricted downloads; effective security information and event management (SIEMS) having the right use cases applied; DOS or DDOS protection service or technology; encryption; and physical or logical networks segmentation Wireless Access Control (Alhayani et al., 2021, p. 4). Often, computer teachers are used as a resource for IT-related issues, but they are not provided specialized training, rather, the responsibility of cybersecurity is de facto left with a very limited number of computer teachers. Effective and evidence-based cybersecurity programs in pre-service teacher training are essential in general and mainly ins STEAM education programs (Pitman, Payne, Vandecar-Burdin & Thorbjornsen, 2022). Very few teachers have the specialized skills and resources required to support digital native students' cybersecurity-related challenges. The government has the responsibility to ensure quality training for teachers, as teachers have the right to work in a safe environment.

Whether the digital environment is seen as a potential threat to or an enabler of children's cybersecurity as their human rights, it can no longer be ignored as a factor in children's well-being and development (Lievens, et.al., 2018). Often, digital natives are better positioned to deal with cybersecurity issues than digital immigrant teachers. Students have higher levels of self-taught technical skills because they have been exposed to technology from a young age, as many students, even at the primary level, have their websites and YouTube channels and are said to be confident users of social media (Pencheva, et.al., 2020). Even though the students have a high level of awareness in certain aspects of using ICT, they lack the basic knowledge of other aspects like password management, phishing, and Two-factor authentication (Garba, et.al, 2020). Thus, the teacher's suggestion to mobilize youth volunteers or young cybersecurity talents as mentors to enhance the school's cybersecurity capacity is relevant.

Students are using more varieties of software and programs than teachers. The students are active users of ICT and online platforms, while most of the senior teachers have less exposure and capacity to provide cybersecurity to the students. Hence, Gen X teachers need additional capacity to handle the students' cybersecurity-related problems. Students' involvement in cybercrime and cyberbullying is common, as some students believe that hacking is glamorous (Pencheva et al., 2020). Creating awareness of how positive peer learning can help youth create a discourse that hacking and engagement (Dahal et al., 2022) in cybersecurity could damage their future as such acts are 'crimes' and will be treated as criminal offenses.

In developing countries like Nepal, cybersecurity is mostly dependent on what security measures are included by the ICT service providers. Schools are not allocating resources for cybersecurity mechanisms. For increased cybersecurity awareness, Dupuis (2017) suggested that, all generational learners get cybersecurity educaiton, so that they are aware of the risks and mitigation measures. The existing policies are useful and comprehensive however, the capacity to implement and follow on of the policies is largely lacking in Nepal. As a result, Nepal has been facing cybersecurity issues such as misusing social media accounts (Roka, 2017). Smeraldi and Malaria (2014) proposed to optimize algorithms to deal with several targets covered by target-specific resources and probably protect students from possible threats. Pencheva et al. (2020) suggested that integrating cybersecurity modules into secondary school education could effectively bridge the intergenerational gap between students, teachers, and parents. This shows the importance of including cybersecurity knowledge and skills in the formal curriculum, enabling students to be more confident about cybersecurity.

Cybersecurity risks are disproportionate among various groups as poor and marginalized children do not have access to cybersecurity awareness as their family members as a result more vulnerable students are perpetrated as well as victimized by cybersecurity risks such as cyberbullying (Liorent, Ortega-Ruiz & Zych, 2016). Similarly, academically low performers and culturally undervalued students are more likely to be 'othered' and experience bullying and harassment (Dhungana, 2021).

Providing a safe space for learning in digital space and providing them digital skills to prevent them from cyberattacks and cyberbullying falls under the principle of the 'best interest of the child of child rights of the CRC. The best interest implies ensuring that technology companies or platform providers consider the best interests of children as children are one of the user groups of their products and services (Lievens et al., 2018). Students in K-12 and teachers may have to find and use various resources and tools such as curriculum, career information, competitions, CyberCamps, etc. The list of such tools is available in Bowen et al. (2022).

Cybersecurity is not the responsibility of a 'computer teacher'; rather, this should be the role of all teachers, school management, local government, and private companies. The state, the duty bearer, needs to invest in cybersecurity and regulate internet service providers. Similarly, it is essential to invest in preparing high-quality cybersecurity professionals. The capacity of the national cyber security workforce is crucial for nations and security organizations (Catal et al., 2022). The intergenerational learning gaps in ICT and cybersecurity can help boost the power of the 'young' to replace the traditional dominance of 'the adult'. This finding is like the idea of making 'cybersecurity talent' (Tsado, 2019). Such talents can use various educational tools, including online games, film and animation, tabletop games, learning modules, and comics, which are expected to be designed using thoughtful instructional design principles and implemented (Zhang-Kennedy & Chiasson, 2021).

Dealing with the negative consequences on the educational performance of many students, particularly in K-12, caused by poor cybersecurity is a serious concern related to a child's right to education. 40% of students' learning is affected by cyberbullying, which must not be ignored. Information professionals should provide students with the necessary skills to ensure safety when they are using the internet (Opesade & Adetona, 2021). Similarly, despite being digital immigrants, teachers are responsible for protecting and promoting children's rights to education and safety. Hence, the state must ivest to increase teachers' cybersecurity capacity in Nepal to ensure access to the internet, rights to education in safe spaces, and the exercise of rights to information. Children's rights are not different when they are online or offline (Kothari, 2019). For educating multi-generational learners, a multi-faceted approach needs to be considered for a successful cybersecurity educational program (Tsado,

2019). This study supported Nasiruddin et.al. (2020), who argued that digital immigrants should make efforts to be part of the digital natives so that they continue to be relevant in the digital era. Lisenbee (2016) suggested using exploration, modeling, scaffolding, classroom problem solving, and independent activities, the EMSCI model, to teach students how to use technology independently and suggested a pedagogical paradigm shift towards constructivist teaching to offset the generation gap.

Further, the school should make efforts in raising awareness to deal with cybersecurity issues, engage young volunteers like cybersecurity talents in helping students increase awareness of cybersecurity, provide parenting education on cybersecurity, and increase teachers' competencies that include developing at least one specialized teacher to deal with cybersecurity challenges, and increase awareness of internet codes of conduct as the state has to provide education in space learning space.

IV. CONCLUSIONS

Making a safe learning environment is a major prerequisite for providing quality education for all in this era where access to the internet and technology is becoming a basic need for all. Creating cyberspace safe for multi-generational learners for both 'native' students as well as 'immigrant' teachers and parents is not prioritized in the least developed countries. While there is a notable cybersecurity awareness and skills gap between students and teachers. Consequently, children's rights to education in a safe and enabling online and offline learning environment have been compromised. Despite having some reasonable policies, because of the teachers' low competencies in cybersecurity, the protection of children from cybersecurity is compromised in Nepal. The students are largely left on their own considering that there is limited practice of a collaborative pedagogical approach. In school, there are no mechanisms to address cybersecurity issues such as a help desk that is easily available for children. Similarly, there are insufficient lessons in the curriculum that could enhance students' cybersecurity capacity and teachers are not trained on this subject matter. More investment to develop tools, teacher training, and curricular and co-curricular activities to promote cybersecurity is essential for quality education. Collaborative pedagogy, which empowers digital natives to take a lead role in cybersecurity by using a problem-solving approach, has the potential to increase digital awareness and skills to cope with the cybersecurity challenges in Nepal. Various cybersecurity measures suggested by the Nepali multi-generational learners are relevant to other similar countries and contexts.

REFERENCES

[1] Acharya, S., & Dahal, S. (2021). Security Threats and Legalities with Digitalization in Nepal. *Research Nepal Journal of Development Studies, 4*(2), 1-15. https://doi.org/10.3126/rnjds.v4i2.42666

[2] Achmad, W. (2021). Citizen and netizen society: The meaning of social change from a technology point of view. *Jurnal Mantik, 5*(3), 1564-1570. https://iocscience.org/ejournal/index.php/mantik/article/view/1663

[3] Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). *Best ways computation intelligent of face cyberattacks.* Best ways computation intelligent of face cyberattacks - ScienceDirect. https://doi.org/10.1016/j.matpr.2021.02.557

[4] Alotaibi, N. B. (2019). Cyber bullying and the expected consequences on the students' academic achievement. *IEEE Access, 7*. https://doi.org/10.1109/ACCESS.2019.2947163

[5] Arora, A., Nandkumar, A., &Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers, 8*(5), 350-362. https://doi.org/10.1007/s10796-006-9012-5

[6] Bowen, D., Jaurez, J., Jones, N., Reid, W., & Simpson, C. (2022). Cybersecurity Educational Resources for K-12. *Journal of Cybersecurity Education, Research and Practice, 2022(1),* 6. Cybersecurity Educational Resources for K-12 (kennesaw.edu)

[7] Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2022). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies,* 1-23. https://doi.org/10.1007/s10639-022-11261-8

[8] Central Bureau of Statistics (CBS), (2011). *Nepal population and housing census, 2011*. Kathmandu: Author. National Population and Housing Census 2011(National Report) – Central Bureau of Statistics (cbs.gov.np)

[9] Choi, M. (2016). A concept analysis of digital citizenship for democratic citizenship education in the internet age. *Theory & research in social education, 44*(4), 565-607. https://doi.org/10.1080/00933104.2016.1210549

[10] Chowdhury, N., & Gkioulos, V. (2021). Cybersecurity training for critical infrastructure protection: A literature review. *Computer science review, 40.* https://doi.org/10.1016/j.cosrev.2021.100361

[11] de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government information quarterly, 34*(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

[12] Dahal, N., Manandhar, N. K., Luitel, L., Luitel, B. C., Pant, B. P., & Shrestha, I. M. (2022). ICT tools for remote teaching and learning mathematics: A proposal for autonomy and engagements. *Advances in Mobile Learning Educational Research, 2*(1), 289-296. https://doi.org/10.25082/AMLER.2022.01.013

[13] Dhungana, R. K. (2018). *Ethnography of school violence: A cultural perspective* (Doctoral dissertation, Kathmandu University). http://dx.doi.org/10.13140/RG.2.2.20521.34405

[14] Dhungana, R. K. (2014). Cyber bullying: An emerging challenge for Nepal. *Pabson review, 7*. (PDF) Cyberbullying: An emerging challenge for Nepal (researchgate.net)

[15] Dupuis, M. J. (2017). Cyber security for everyone: An introductory course for non-technical majors. *Journal of Cybersecurity Education, Research and Practice, 2017*(1), 3. Cyber Security for Everyone: An Introductory Course for Non-Technical Majors (kennesaw.edu)

[16] Fees, R. E., Da Rosa, J. A., Durkin, S. S., Murray, M. M., & Moran, A. L. (2018). Unplugged cybersecurity: An approach for bringing computer science into the classroom. *International Journal of Computer Science Education in Schools, 2*(1), 3-13. Doi. https://doi.org/10.21585/ijcses.v2i1.21

[17] Florek, I., & Eroglu, S. E. (2019). The need for protection of human rights in cyberspace. *Journal of Modern Science, 42*(3), 27-36. https://doi.org/10.13166/jms/112765

[18] Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: *A quantitative approach. Int. J. Emerg. Technol, 11*(5), 41-49. A_Study_on_Cybersecurity_Awareness-libre.pdf (d1wqtxts1xzle7.cloudfront.net)

[19] Giri, S., & Shakya, S. (2020). High risk of cybercrime, threat, attack and future challenges in Nepal. *International Journal of Computer Sciences and Engineering, 8*(2), 46-51. https://doi.org/10.26438/ijcse/v8i2.4651

[20] GoN, 2019. *Digital Nepal framework 2019*. Kathmandu: Government of Nepal, Ministry of Information, Communication: Kathmandu. D8lp6S0TBu0kqwXB7V90hB9aodF4v6qTLGzUvN7M.pdf (drc.gov.np)

[21] GoN, 2020. *Cyber security bylaw 2077*, (2020). Nepal Telecommunication Authority: Kathmandu. Cyber-Security-Bylaw-2077-2020.pdf (nta.gov.np)

[22] GoN, 2021. *Online Child Protection Procedure 2021*. Kathmandu: Ministry of Women, Children, and Senior Citizens. Online_Child_Protection_Asar_31.pdf (mowcsc.gov.np)

[23] International Telecommunication Union (ITU), 2020. *Global cybersecurity index 2020*. Global Cybersecurity Index (itu.int)

[24] ITU (2008). *Series X, data networks, open system communications and security, telecommunication security: Overview of cybersecurity*. X.1205 : Overview of cybersecurity (itu.int)

[25] Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education, 18*(3), 1-12. https://doi.org/10.1145/3152893

[26] Leite-Trambly, O., & Obasi, S. N. (2018). *Five Generations: Preparing multiple generations of learners for a multi-generational workforce*. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1005&context=ipts

[27] Llorent, V. J., Ortega-Ruiz, R., & Zych, I. (2016). Bullying and cyberbullying in minorities: Are they more vulnerable than the majority group?. *Frontiers in psychology*, *7*, *1507*. https://doi.org/10.3389/fpsyg.2016.01507

[28] Lisenbee, P. (2016). Generation gap between students' needs and teachers' use of technology in classrooms. *Journal of Literacy and Technology*, *17*(3). JLT_V16_3_v2 (literacyandtechnology.org)

[29] Lievens, E., Livingstone, S., McLaughlin, S., O'Neill, B., & Verdoodt, V. (2018). Children's rights and digital technologies. *International human rights of children*, *1*, 27. http://doi.org/10.1007/978-981-10-4184-6_16

[30] Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New media & society*, *19*(5), 657-670. https://doi.org/10.1177/1461444816686318

[31] Ministry of Education, Science and Technology (MoEST), (2019). Comprehensive school safety implementation guidelines. Kathmandu: Author 65374_cssimplementationguidelineswithendc.pdf (preventionweb.net)

[32] Moise, A. C. (2016). Cybersecurity and Human Rights. *Rev. Universul Juridic*, 160. Cybersecurity and human rights.pdf (jandmparker.net)

[33] Mohr, K. A., & Mohr, E. S. (2017). Understanding generation Z students to promote a contemporary learning environment. *Journal on empowering teaching excellence*, *1*(1), 9. https://doi.org/10.15142/T3M05T

[34] Nepal Police, 2022. *Cyber bureau.* Introduction - cib.nepalpolice.gov.np

[35] Nepal telecommunication authority (NTA), 2021. *MIS report, Baisakh, 2079* (14 April 2022– 14 May 2022). MIS-Baisakh-2079.pdf (nta.gov.np)

[36] Nepal telecommunication authority (NTA), 2021. *Annual report 2021*. https://nta.gov.np/annualreport

[37] Nepal telecommunication authority (NTA), 2019. *Online Child Safety Guidelines 2019*. Online-Child-Safety-Guidelines-2076.pdf (nta.gov.np)

[38] Opesade Dr, A. O., & Adetona Mr, A. O. (2021). An Assessment of Internet Use and Cyber-risk Prevalence among Students in Selected Nigerian Secondary Schools. *Journal of Cybersecurity Education, Research and Practice*, *2020*(2), 3. "Internet Use and Cyber-risk Prevalence" by Adeola O. Opesade Dr and Abiodun O. Adetona Mr (kennesaw.edu)

[39] Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68-74. http://dx.doi.org/10.1109/MSEC.2020.2969409

[40] Phyak, P., Gurung, Y., Khanal, P. & Mabuhang, B.K., (2019). The Existing situation of digital literacy and use of ICT in public secondary schools: A baseline study. Existing Situation of Digital Literacy and Use of ICT in Public Secondary Schools (britishcouncil.org.np)

[41] Prensky, M. (2001). Digital natives, digital immigrants part 2: Do they really think differently? On the horizon. *Industrial and commercial training*,*43*(7). 460-466. https://doi:10.1108/00197851111171890

[42] Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International journal of child-computer interaction*, *30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

[43] Radhakrishnan, K., Angrist, N., Bergman, P., Cullen, C. Matsheng, M., Ramakrishnan, A., Sabarwal S., Sharma, U. (2021). *Learning in the time of covid 19: Insights from Nepal*. World Bank Document

[44] Rajbhandari, J., & Rana, K. (2022). Cyberbullying on social media: an Analysis of teachers' unheard voices and coping strategies in Nepal. *International journal of bullying prevention*, 1-13. https://doi.org/10.1007/s42380-022-00121-1

[45] Rana, K., & Rana, K. (2020). ICT Integration in Teaching and Learning Activities in Higher Education: A Case Study of Nepal's Teacher Education. *Malaysian Online Journal of Educational Technology*, *8*(1), 36-47. http://dx.doi.org/10.17220/mojet.2020.01.003

[46] Reed, K. P., Cooper, R. L., Nugent, W. R., & Russell, K. (2016). Cyberbullying: A literature review of its relationship to adolescent depression and current intervention strategies. *Journal of Human Behavior in the Social Environment*, *26*(1), 37-45. https://doi.org/10.1080/10911359.2015.1059165

[47] Roka, C. B. (2017). Cybercrime and security in Nepal: The need for two-factor authentication in social media. Crossing the border: *International Journal of Interdisciplinary Studies*, *5*(2), 31-36. https://doi.org/10.3126/ctbijis.v5i2.18436

[48] Rona, G., & Aarons, L. (2015). State responsibility to respect, protect and fulfill human rights obligations in cyberspace. *Journal of national security law and policy*, *8*, 503. https://ssrn.com/abstract=2859615

[49] Saud, M. S. (2021). Digital literacy competencies among English teachers of Nepal: Are they ready for online instruction? *Malaysian online journal of educational technology*, *9*(4), 1-13. http://dx.doi.org/10.52380/mojet.2021.9.4.204

[50] Secretariat, C. A., & Durbar, S. (2015). Constitution of Nepal 2015. *Kathmandu: Constituent Assembly Secretariat*. Nepal_2015.pdf (constituteproject.org)

[51] Smeraldi, F., & Malacaria, P. (2014, May). How to spend it: optimal investment for cyber security. *In Proceedings of the 1st International workshop on agents and cybersecurity*,1-4. https://doi.org/10.1145/2602945.2602952

[52] Solms, V. R., & Solms, V. S., (2015). *Cyber safety education in developing countries.* ISSN: 1690-452. download (psu.edu)

[53] Tsado, Lucy (2019) "Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach," *Journal of cybersecurity education, research and practice, 1*(4). https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/4

[54] United Nations (UN). (1989). *Convention on the rights of the child*. Treaty Series, 1577, 3. Convention on the Rights of the Child (wunrn.org)

[55] Yawson, D. E., & Yamoah, F. A. (2020). Understanding satisfaction essentials of e-learning in higher education: A multi-generational cohort perspective. *Heliyon*, *6*(11), e05519. https://doi.org/10.1016/j.heliyon.2020.e05519

[56] Yuliana, Y. (2022). The importance of cybersecurity awareness for children. *Lampung Journal of International Law*, *4*(1), 41-48. https://doi.org/10.25041/lajil.v4i1.2526

[57] Zulkifli, Z., Molok, N. N. A., Abd Rahim, N. H., & Talib, S. (2020). Cyber security awareness among secondary school students in Malaysia. *Journal of information systems and digital technologies*, *2*(2), 28-41. https://journals.iium.edu.my/kict/index.php/jisdt/article/view/151

[58] Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1-39. https://doi.org/10.1145/3427920

V. Appendix 1: Survey Questionnaire

A. Survey Question for School teachers teaching online/distance mode

We believe that your classroom and teaching are changing due to the increased use of the internet and technologies. Most of you are fully or partly using online classes and learning during the Covid 19 pandemic. Many of you may be facing different challenges including your safety and security issues. We are carrying out an independent study to understand your challenges related to internet safety and making students like you safe from cyber-related risks. For this purpose, we request you help us by participating in this survey. We assure you that your identity will not be disclosed, and your valuable information will be used only for academic purposes Participating in this survey is safe. You will have to spend 10-12 minutes completing this survey.

Introductory Information

1.	Name (Optional)	
2.	Sex	Male …... Female ……..Others……...
3.	Age	……..years
4.	Internet Access	Do you have private wifi at home? _____ Do you use mobile data? _____ Do you use the internet on sharing basis? _____ Do you use public wifi wherever available? _____
5	Online resources/Social Media	What online resources or social media do you use? Blogs ____ Websites _____ Youtube _____ Facebook _____ Instagram _____ Snapchat _____ Others _____
6.	Computer Skills	Basic_____ Advanced Professional_____
7	Training	Trained in Digital Pedagogy Received very little orientation on digital pedagogy Not trained on digital pedagogy
8	Training on Cyber Security	Trained in Cyber security Received very little orientation on cyber security Not trained in cyber security

Knowledge About Cyber Security Related Risks

S.N	Questions	Yes	No
1.	Have you heard about cyber security?		
2.	Do you have prior knowledge in cyber-crime and cyber-bullying?		
3	Have you installed an anti-virus program on your computer and updated regularly?		
4.	Do you know that some students send or receive offensive messages, and their rumours are spread and humiliated in social media?		
5.	Do you know that children can easily become a victim of cyberbully?		
6	Do you feel confident to help students deal with their cybersecurity issues?		

Cyber-Security Related Skills

SN	Statements	Never	Some times	Often
1.	I do not share my password with my friends.			
2.	I use different passwords across different websites and accounts.			
3.	I do not respond to stranger's messages, video chat, or their friend request.			
4.	I check for viruses whenever I download any files.			
5.	I give attention to the privacy settings on your social media such as Facebook.			
6.	I use strong passwords (consistent, lowercase, uppercase, numbers, and special characters) and change them periodically.			

Attitude and Mitigation Measures

SN	Statements	Never	Some times	Often
1.	I feel much better to post funny pictures/videos of my friends in public and sending annoying messages online.			
2.	My personal information has no value to the hackers so I don't think they will target me.			
3.	I click on the advertisements or pop-up screens that appear when surfing the internet.			
4.	I believe that no one will send me anything malicious, scams through emails or annoying pictures and texts.			
5.	I have reported inappropriate post on social media.			

Netizenship Or Netiquette Behaviour

SN	Statements	Never	Some times	Often
1	I understand the internet codes of conduct and follow them			

2	I am reminded about the right internet behaviour by the school			
3	I received sufficient orientation about the legal consequences of not following internet codes of conduct			
4	I report any activities that have safety or security issues to my school			
5	I have reported internet safety related to issues with teachers			
6	I have discussed internet safety-related issues with my family members			

Cyber Security Support System

SN	Statements	Never	Some times	Often
1.	Do you believe that you get the necessary support for your cyber security from your school?			
2.	Do you believe that your teachers are competent to help in your cyber security issues if occurred?			
3.	Do you believe that your school system is well-resourced to help you in your cyber security issues if occurred?			
4.	Are you aware of any policies formulated by the government to help withs your cyber security issues, if occurred?			
5.	Are you aware of any institutions established by the government to help with your cyber security issues, if occurred?			

Do you have any suggestions to make your digital learning safe?

Pls specify…….

B. *Appendix 2: Key Information Interview Schedule for Teachers*

- How have the Z Generation learners (born after 2010) experienced cyber security issues in their online learning space?
- What are the cyber security issues reported by students and experienced by teachers?
- Any issues and challenges they experience related to different generations of learners?
- How are they dealing with cyber security issues?
- How are the X Generation teachers (Born before 2000) making cyberspace safe for the Z Generation learners?
- Any examples of cyber security issues experienced by teachers?
- How have they responded to cybersecurity-related issues?
- Competencies – knowledge, skills, and resources they have to deal with cyber security issues?
- What are the consequences of poor cyber security in the increasing digital learning space?
- What consequences to the students? Bullying, Harassment, Distraction
- What consequences to the teachers? Same as above
- Consequences to learning? It negatively impacts learning.