Cybersecurity Awareness Amongst Youth – A Survey in Delhi/NCR

Vaishali Chawla [1], *Yatin Kapoor* [2] *and Tanya Chawla* [3]

Abstract

Cyberspace has become an integral part of modern society, especially in the last two decades. As the internet has rapidly progressed globally, the community of cyber users in cyberspace has widely expanded. One group of cyber users that is swiftly becoming active in cyberspace is the youth, particularly, school and college students. However, young cyber users are increasingly becoming the soft targets of cybercriminals. Taking cognizance of the rising cybercrime cases against young cyber users, this research study surveyed several schools and colleges in the Delhi-NCR region to assess the cyber awareness among students and academic professionals. It was found that most of the participants were not aware of ethical and safe digital practices. These observations are attributed to the poor application of initiatives to ensure cyber safety among school children, especially in developing countries like India. Based on the findings from the survey, this study provides suggestions and recommendations to various role-players involved in cyberspace to assure safe cyber behaviour.

Keywords : **Cyber awareness, Cybersecurity, Cyberspace, Education survey, Delhi/NCR, Indian youth**

I. INTRODUCTION

With the advent of the internet, the number of users entering cyberspace has been increasing worldwide [1]. Cyberspace is defined as an environment in which users communicate and connect via a network with other users across the globe. Users who use the internet to connect to cyberspace are called cyber users [2]. Cyberspace has become an indispensable part of our lives. From patients receiving consultations by medical practitioners over a video call to students conveniently giving exams from their places to professionals working from home, cyberspace has rapidly expanded. Nowadays, cyber users range in age, gender, nationality, and geographical location, surpassing linguistic and demographic barriers. Alas, the extensive growth in cyberspace has reached the hands of online predators such as hackers and child groomers who leverage these technologies for their malicious intentions and ill will [3].

While anyone using technology is at equal risk, a study concluded that children represent the most vulnerable sections of society and get easily exploited in cyberspace [4]. Furthermore, researchers have established that school learners are immensely prone to cyber threats [5], [6]. The situation is alarming for India as at least one cybercrime was reported every 10 minutes in the first six months of 2017 [7]. Such numbers are of serious concern, especially in a young nation like India, where partial or little awareness exists about cybersecurity in young internet users. Hence, it becomes

Paper Submission Date : March 5, 2023 ; Paper sent back for Revision : March 10, 2023 ; Paper Acceptance Date : March 12, 2023; Paper Published Online : April 5, 2023

[1] V. Chawla (*Corresponding Author*), *Ex-Student*, Department of Computer Science, University of Delhi, New Delhi - 110 007, India. Email : vaishali.mcs18.du@gmail.com ; ORCID iD : https://orcid.org/0000-0002-9181-8179

[2] Y. Kapoor, *Ex-Student*, Department of Computer Science, University of Delhi, New Delhi - 110 007, India. Email : yatin.mcs19.du@gmail.com ; ORCID iD : https://orcid.org/0000-0003-3932-9017

[3] T. Chawla, *Ex-Student*, Department of Computer Science, Atma Ram Sanatan Dharma College, University of Delhi, New Delhi - 110 021, India. Email : tanyachawla104@gmail.com ; ORCID iD : https://orcid.org/0009-0007-7594-0784

DOI : https://doi.org/10.17010/ijcs/2023/v8/i2/172777

crucial to understand cybersecurity awareness in learners and devise strategies to control the increasing cybercrime cases against them. Therefore, this study addresses the need to instill safe, sound, and ethical cyber practices in users from a very early stage of learning. A specific survey was conducted across numerous schools and colleges in the Delhi-NCR region to assess cybersecurity awareness among learners and academic professionals. Institutions of learning involve various stakeholders in addition to learners such as parents, faculty, school management and administration, and concerned government organizations. Each stakeholder has a role to play in cyberspace and groom the learner to become digitally safe. Consequently, the study also presents some suggestions and recommendations to each of the concerned stakeholders in a bid to make cyberspace more secure.

The key contributions of this research work can be summarized as follows:

1) Reviewing the work done in cybersecurity awareness among children at the global level and scrutinizing the strategies and approaches suggested by previous studies in the field.

2) Surveying various schools, colleges, and institutions of learning and analyzing the participants' responses to assess the current level and status of cyber awareness.

3) Presenting suggestions and recommendations to concerned stakeholders that can help check cyber incidents among the users, especially children.

The remainder of the paper is structured as follows: Section II aims to review the work done in the field, while Section III elucidates the design of the survey conducted for this study. Section IV presents a summary of the observations made form survey responses. Finally, Section V concludes the paper.

II. LITERATURE REVIEW

Cybersecurity has been a trending topic of research and discussion, specifically during the last decade. Globally, much research has been directed towards cybersecurity awareness; however, research for cybersecurity among children is still in its inflexion phase. A study [8] was performed to examine the effectiveness of the cybersecurity awareness program provided by the Ministry of Education in UAE for students aged 8 to 10 years. It was observed that the children are more at risk while online, and cybersecurity awareness is essential. Some researchers [9] have examined the various kinds of online risks children are exposed to in cyberspace. The study concluded that the chances of getting exposed to online risk are much higher for younger learners. School learners across the globe have been easy targets of cyber criminals [10], [11]. Several studies have performed a quantitative investigation to highlight the gravity of the situation. It has been recorded that 94% of children aged 3 to 18 have a computer at home, while 61 % additionally have internet access [12]. A recent survey revealed that 40% of children in grades 4-8 have talked to a stranger online, 53% provided their phone number, 30% texted, and 15% tried to meet up with unknown individuals [13]. These numbers reflect a distressing situation.

Various surveys and researches have been conducted recently, particularly in the Indian context [14–17] to assess the cyber awareness of school learners and graduate students. These studies have also suggested measures to ameliorate the cybersecurity awareness among naïve cyber users. According to the research study [18] conducted in India for 5 years, 81% of children aged 8 to 16 are already active on social media. Nearly 77% of these children had a Facebook account before they were 13 years of age. Almost one in five children face online abuse. A global survey [19] conducted by Microsoft ranked India third in cyber-bullying, with 53% of the respondents, primarily children experiencing cybercrime and exploitation in cyberspace. Consequently, these studies conjointly indicate an alarming situation in India. The research community and academia need to collaborate and initiate effective measures to address this challenging state of affairs. One of the viable solutions is to include cybersecurity as a dedicated element of curriculum in all disciplines across schools, colleges, and institutions of learning.

The unexpected global pandemic of COVID-19 confined people to their homes. This also led to a drastic shift in the traditional educational paradigm in India [20]. The use of ICT tools proved to be of great help in imparting and imbibing knowledge. The author in [21] has highlighted the issue of inevitable exposure and vulnerability of children in the cyberspace. While some studies [22] have been conducted in a similar context, there was a lack of recent survey-based studies in India.

III. SURVEY DESIGN

Addressing the need of a specific survey-based study of the level of cyber awareness in Indian children and youth, a survey was designed and this section elaborates that process.

A. Data Collection

In this study, the method used for data collection was an online survey. The survey was conducted across various schools and colleges in the Delhi-NCR region employing the simple random sampling method [23]. Responses of the participants were collected through the questionnaire method. The purpose, importance, and significance of the study were clearly described to all the participants. Adhering to the privacy guidelines [24], no personally identifiable or confidential information was collected. Due diligence was performed while conducting the survey, consent was taken from the participants before recording their responses. Participation in the survey was completely voluntary. The data collected via survey were solely used within the purview of this research. Conforming to the objectives and scope of this study, a set of 19 carefully crafted, rudimentary questions were included in the survey. The survey consisted of two sections: Section A and Section B. The former section comprises 16 questions on the daily interaction of the users with cyberspace. The questions in this section were used to assess the level of awareness or digital literacy among the participants. The next section consisted of 3 questions targeted only at the educators and the responders who were professionally associated with academia. The questions in this section were related to the course structure and important topics of cybersecurity that should be included in the school curriculum.

B. Survey Participation

To ensure a diverse background and rich quality of responses, the survey encouraged participation from learners, educators, research scholars, readers, professors, and management and administration of academia. Among the learners, the highest academic qualification encompasses senior school (Class X) pass out, senior secondary (Class XII) pass out, graduation, post-graduation, and doctorate.

C. Storing the Responses

After receiving the responses from the participants, the responses are stored and conditionally saved into databases. As per the design specifications of the survey, Section A was a common section to assess the level of cyber awareness of the participants and identify potentially weak areas, whereas Section B pertains to only the educators or those associated with the field of academia who can provide valuable insights and opinions on the important topics and course structure of the cybersecurity subject to be included in the school curriculum. Therefore, two separate databases are leveraged, one each for Section A and B. Subsequently, data analysis was performed on the saved responses.

D. Data Analysis

A much significant task of any survey process is to perform rigorous and comprehensive data analysis. The purpose of data analysis is to inspect, describe, and discover useful findings from the data. Various statistical and data visualization techniques are employed to achieve the stated purpose, and the findings from the recorded responses are elucidated in Section IV.

E. Reliability of the survey

The reliability of this survey was determined using the test-retest technique [25]. This technique measures the difference in the responses of individuals recorded at two different time instances. This technique is widely used in establishing the reliability of a questionnaire. The same questionnaire was presented to the respondents twice, at T1 and T2, four months apart. Responses corresponding to each question were quantified on a scale of 1 to 3. The sum of scores of responses by each individual was noted at both, T1 and T2. Scores of respondents at T1 and T2 were then compared by computing the Pearson Correlation Coefficient [26]. The value of correlation coefficient is directly proportional to the reliability of the survey. The value of Pearson Correlation Coefficient was 0.859 for this survey.

IV. RESULTS AND ANALYSIS

This section presents the experimental setup of the undertaken research study. The online survey used for

TABLE I.

HIGHEST ACADEMIC QUALIFICATION AND AGE OF THE SURVEY PARTICIPANTS

Highest Academic Qualification	Number of Participants	Age	Number of Participants
Senior school (class X)	147	11–13	138
Senior secondary (class XII)	180	14–16	243
Graduation	129	17–19	147
Post-Graduation	117	20–24	54
Doctorate	27	≥25	18
Other	18	–	–

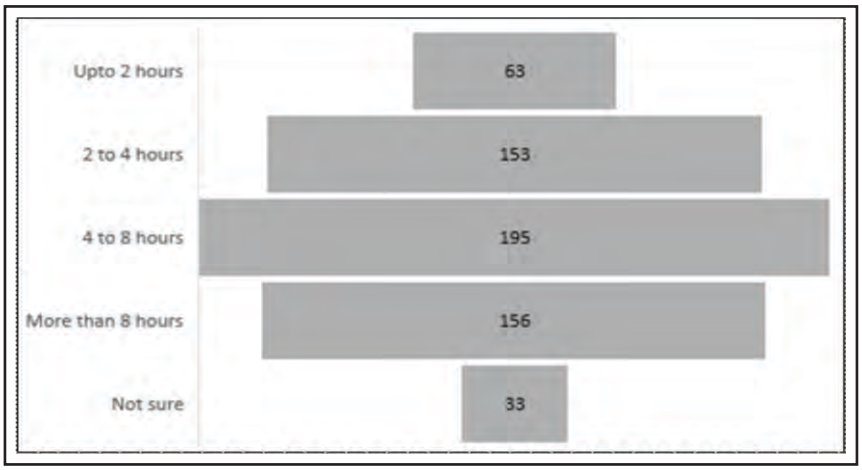


Fig. 1. Average daily internet usage of the survey participants

data gathering was designed via *Google Forms*[1], providing an easy-to-use interface with quick response collection and analysis. The survey invitation was sent via email to competent authorities of various schools and colleges of the Delhi-NCR region. The survey consisted of sections A and B, intended for different target audiences (refer sub-section A of section III). Section A consisted of 16 questions, while Section B consisted of three questions.

Altogether 600 participants responded to the survey, out of which 90 participants were associated with academia either as an educator or via administration or management. The survey also recorded age and highest academic qualification attribute to have a wider perspective in the response recorded and the confidence associated with it. The ratio of female to male participation in the survey was 55% and 45%. Table I summarizes the distribution of the highest academic qualification and age attribute of the survey participants.

It is noteworthy to mention that the number of responses recorded for Section A and Section B were 600 and 90, respectively. Only 90 participants who were professionally associated with academia were eligible to fill Section B of the survey.

A. Survey Section A : Observations

This subsection describes the conclusions and findings from Section A of the online survey. The participants were requested to fill in their average number of daily hours on the internet, including social media, surfing, and gaming (Fig. 1). It was observed that nearly one in three participants spent upto 8 hours, whereas one in four participants spent more than 8 hours on the internet on a day-to-day basis.

The survey participants were asked if they ensure the complete know-how of any electronic device or a web

[1] https://www.google.com/forms/about/

TABLE II.

RESPONSES OF THE SURVEY PARTICIPANTS ON RECEIVING PHISHING EMAILS

Have you ever received a phishing email?	Number of responses
Yes, I regularly receive such emails	252
No, I have never received such emails	264
I don't know what that means	84

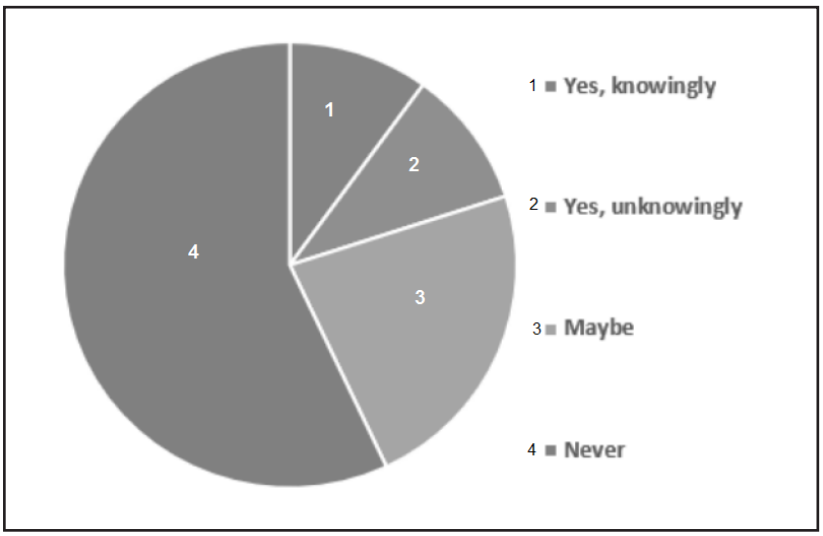


Fig. 2. Responses of the survey participants on sharing of personal or confidential information

page or an application before using it. It was observed that only about 37% of the participants claimed to make themselves familiar with the policies, guidelines and details of a gadget before using it. Around 15% of the participants reported that their social media accounts have been hacked one or more times.

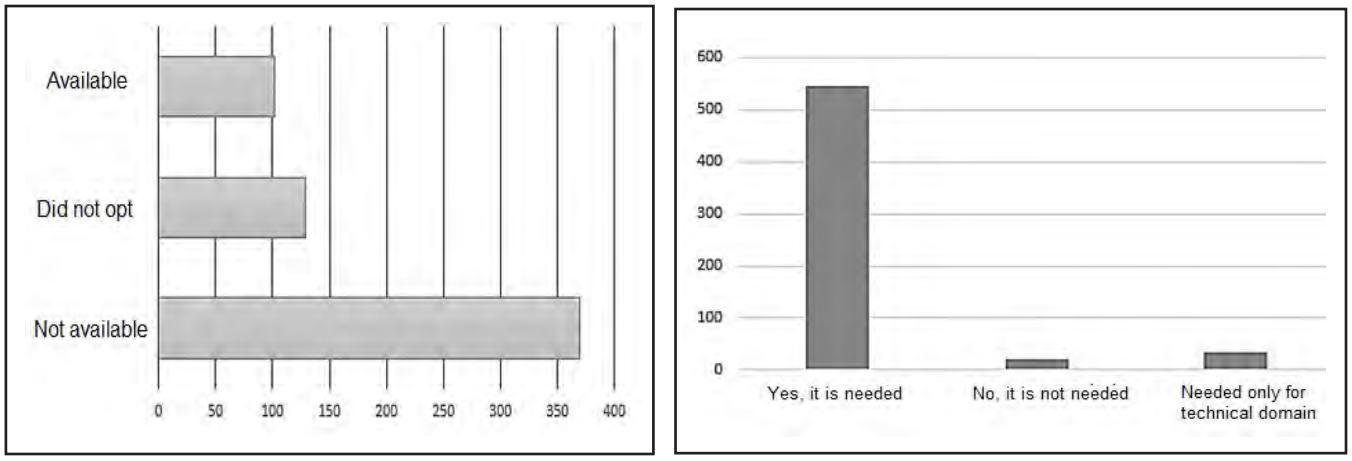
As shown in Table II, 42% of the respondents received phishing emails on a daily basis, while 14% were unaware of what a phishing email means. One in five participants agreed that they have knowingly or unknowingly shared personal and confidential details over a phone call or a website or while playing online games, while 23% of the participants were not sure if the nature of details shared by them was confidential or sensitive (Fig. 2). Furthermore, 10% of the participants admitted being victims of cyber bullying, while 5% were unsure about it. The indecisiveness of the participants indicates a grave lack of awareness and vigilance.

Consequently, the participants were asked if they knew how to deal with situations involving cyber crimes such as hacking, fraud due to phishing emails, cyber bullying, harassment, social engineering attacks, among others, and whether or not they had awareness about the Indian cyber laws such as the IT Act, 2000 and IT Amendment Act, 2008. It was distressingly observed that only 22% of the participants had some knowledge of the cyber laws, while as many as 58% had never heard of any cyber law that regulates the cyberspace. 20% of the responders did not know what to do and who to contact if they become victims of cybercrime, while 56% reported that they merely ignore phishing emails and never report ? It was recorded that around 47% of the participants are more likely to visit a url beginning with http rather than https. Among this fraction of participants, most of them find no difference between http and https. Further, from a list of online activities, the participants were asked to select which one (or more) according to them would be classified as a cybercrime. The responses recorded for this question are summarized in Table III. A small fraction of 2% respondents who thought that neither of these

TABLE III.

RESPONSES OF THE SURVEY PARTICIPANTS ON WHAT ACTION IS CONSIDERED AS CYBERCRIME AS PER THEIR KNOWLEDGE

Which of the following is a cybercrime?	Number of responses
Downloading media from blocked URLs or Torrents	378
Posting morphed pictures of people on social media	510
Making a profile on the internet using someone else's details	549
Sharing your password with others	135
Relentlessly messaging people	264
None of the these	12



(a) (b)

Fig. 3. Response of the survey participants on (a) Availability of Cybersecurity in the Curriculum, and (b) Whether introducing the subject in the curriculum would impart the adequate knowledge to ensure safety in the Cyberspace

activities was a cybercrime highlights a dismal state of affairs.

Majority of the participants confirmed that they used a strong password, that is, a combination of characters, digits and special characters. Only 8% of the participants frequently changed their passwords, while over 33% never changed their passwords. A study by cybersecurity firm Delinea revealed that 4 out of 5 cybersecurity attacks involved a weak or stolen password. Regularly changing passwords can provide an extra layer of protection against many potential attacks.

Additionally, the participants were asked if they had studied cybersecurity as part of their curriculum and whether including cybersecurity in the curriculum would provide adequate knowledge to make them more secure in cyberspace. Both the scenarios are shown in Fig. 3 (a) and (b). It can be seen that almost 62% of the participants had not studied cyber security due to its academic unavailability. However, 91% of the participants thought that including cybersecurity in the curriculum would prove beneficial.

It is perspicuously evident that most participants failed to depict secure cyber behaviour when interacting with cyberspace. The lack of awareness of the concerned cyber laws and know-hows of reporting cybercrime is a major concern.

B. Survey Section B : Observations

This subsection presents the responses recorded for Section B of the online survey. A total of 90 responders, professionally associated with academia were eligible to participate in Section B of the survey. The questions included in Section B pertain to the overall course

TABLE IV.

RESPONSES OF THE PARTICIPANTS ON WHETHER NEP 2020 WOULD FACILITATE THE INTRODUCTION OF CYBERSECURITY IN THE SCHOOL CURRICULUM IN INDIA

Will NEP 2020 suffice in instilling cyber awareness among learners right from school?	Number of responses
Yes	45
No	12
Not very clear about implementation details of NEP 2020 yet	33

Fig. 4. Word Cloud of the list of topics that should be included while designing a course structure for cybersecurity, as responded by the academic professionals

structure and important topics that should be included as a prospectus for the subject.

The academic professionals were enquired if they sensed the need for a subject devoted to cyber security in the curriculum. 84 out of 90 participants responded positively to this question. The National Education Policy (NEP) [27] introduced by the government of India in 2020 plans to transform the previous static curriculum into a dynamic curriculum employing an interdisciplinary approach. The policy aims to make the curriculum skill based by allowing students to opt for subjects of their choice even if they do not conventionally come under the purview of their pursuing stream. The standpoint of the academic professionals on the same was also enquired and the responses are shown in Table IV.

Last, the survey prompted the academic professionals to enlist the topics covered under cyber security subject if they were to design its course structure. The responses recorded from this question are depicted via a word cloud [28] (Fig. 4).

C. Other Important Findings

This section presents certain crucial and alarming observations drawn from the survey. The following observations are enlisted on the basis of gender, qualification level and age.

- Across all age groups, 1 in every 10 female respondents has fallen prey to cyber bullying.
- Male participants reported spending a greater share of their time online as compared to the female counterparts. About 1 out of every 3 males spent more than 8 hours on the internet on a daily basis.
- Out of the 27 respondents with a Ph.D. qualification, 24 were unaware of the know-how of reporting a cybercrime.
- At least 1 in every 5 respondents between 11 to 15 years of age has shared his/her password online.
- Almost half of the respondents who claimed that their account was hacked had never changed their passwords.

↳ Of the 198 respondents who didn't know where to report a cybercrime, 165 (or 83.33%) declined having knowledge about cyber laws.

D. Suggestions to Concerned Stakeholders

In addition to the learners, participation from the government, educational institutions, teachers, and parents will play a vital role in achieving digital safety. Based on the authors' reflection on the current status of cyber security awareness and the findings from the survey, this section suggests some measures for the concerned stakeholders.

1) Recommendations for the Government

↳ The government may consider strengthening the existing cyber laws and take initiatives to make the common citizens including children aware of their rights in cyberspace.

↳ A centralized monitoring system for the protection of young children in cyberspace is also recommended. Special cells that cater to counselling children who have been victims of cyber crimes could be established or integrated with not-for-profit organizations already providing mental health counselling and therapy.

↳ Developing, promoting, and conducting awareness programs and workshops that highlight the importance of becoming a safe netizen will prove beneficial in the long run. Mass media, print media, and digital media can also be leveraged to achieve this goal.

2) Ideas for Educational Institutions and Academic Professionals

↳ Academic institutions may organize cyber safety training camps, boot camps, workshops, and seminars by subject matter experts for students, teachers, and parents.

↳ A committee in charge of issues related to cyberspace may be formed at the institution level. This committee may decide upon rules that restrict potentially unsafe internet activity. Additionally, it may handle situations where a student is a victim or when a student is found to have committed an undesirable act in cyberspace.

↳ The emotional quotient of cyber users should also be addressed. Due to lack of maturity, cybercrime situations such as cyber bullying, cyber defamation, derogatory comments, and trolling affects the students, especially young learners mentally. Hence, counselling sessions for such students can also be arranged by the institution.

↳ Merely incorporating cyber security as a subject may limit its prospect to scoring marks. Theoretical knowledge should be supplemented with hands-on experiences such as, mock drills and state-of-the-art lab facilities to fully realize cyber-safe behaviour.

3) Suggestions for Parents

↳ Parents should actively participate in awareness campaigns.

↳ Any apprehensions about the child's behaviour should be discussed with teachers or counsellors without fail.

↳ Parents should consider referring to an expert before buying any software, hardware or internet-related subscription for very young children.

4) Advice to Children and Individuals

↳ Children should be made to learn to be vocal about their insecurities and trepidations that might be a consequence of cyber risk or attack. They should not be hesitant in discussing and reporting any unpleasant experience on the internet.

↳ One must recognize the potential threats that can occur while interacting with a stranger in cyberspace.

↳ Young internet users should attend workshops, seminars, orientations, and training sessions concerning cybersecurity awareness and keep updating themselves with the latest advancements in this field.

V. CONCLUSION

An online survey was conducted among several schools and colleges of the Delhi-NCR region. A total of 600 participants including students, teachers, research scholars, readers, professors, administration, and management professionals responded to the survey. The survey analysis showed that the level of cyber awareness is below par for the majority of the participants, which puts them in a threatening situation in the digital space. It is an alarming concern given the rapidly increasing dependence on cyberspace. Therefore, across all

disciplines there is a need to introduce a subject devoted to cybersecurity with an interactive and creative pedagogical style to ensure a safe and secure cyberspace experience for the users. The study also provides suggestions and recommendations to the concerned stakeholders of cyberspace to ensure safe cyber behaviour in the online world.

AUTHORS' CONTRIBUTION

Vaishali Chawla and Yatin Kapoor ideated the study. Yatin Kapoor and Tanya Chawla worked on the literature review. All the three authors worked on the design and circulation of the survey. Tanya Chawla cleaned and managed the responses. Yatin Kapoor and Vaishali Chawla performed data analysis and drew observations. All authors jointly finalized the article.

CONFLICT OF INTEREST

The authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in the manuscript.

FUNDING ACKNOWLEDGEMENT

The authors have not received any financial support for the research, authorship, and/or for the publication of the article.

REFERENCES

[1] "Number of internet users worldwide from 2005 – 2019 (in millions)." Statista.com. Accessed: Jun. 1, 2021. [Online]. Available: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[2] E. Kritzinger, "Improving cybersafety maturity of South African schools," *Inf.*, vol. 11, no. 10, 2020, doi: 10.3390/info11100471.

[3] Symantec, "Internet Security Threat Report," vol. 21, 2016. [Online]. Available: https://docs.broadcom.com/doc/istr-21-2016-en

[4] S. Kumar, "Crime against children in cyber world," *J. Contemp. Issues Law*, vol. 5, no. January, 2021.

[5] M. F. Wright, "Adolescents' cyber aggression perpetration and cyber victimization: The longitudinal associations with school functioning," *Soc. Psychol. Educ.*, vol. 18, pp. 653–666, 2015, doi: 10.1007/s11218-015-9318-6.

[6] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *Int. J. Inf. Educ. Technol.*, vol. 10, no. 5, pp. 378–382, 2020, doi: 10.18178/ijiet.2020.10.5.1393.

[7] R. D. Tiwari, "An analytical study on the awareness of parents about cybercrimes against children," *Int. J. Transform. Media, Journalism Mass Commuication*, vol. 4, no. 2, 2019. [Online]. Available: http://management.eurekajournals.com/index.php/IJTMJMC/article/view/332

[8] A. A. Al Shamsi, "Effectiveness of cyber security awareness program for young children: A case study in UAE," *Int. J. Inf. Technol. Lang. Stud.*, vol. 3, no. 2, pp. 8–29, 2019, doi: 10.13140/RG.2.2.28488.14083.

[9] S. Livingstone, G. Mascheroni, and E. Staksrud, "Developing a framework for researching children's online risks and opportunities in Europe." EU Kids Online, no. November, pp. 1–21, 2015. [Online]. Available: http://eprints.lse.ac.uk/64470/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU%20Kids%20Online_Developing%20framework%20for%20researching_2015.pdf

[10] J. S. Srivastava, "Cyber crime: Kids as soft targets," *Int. J. Innov. Comput. Sci. Eng.*, vol. 4, no. 1, pp. 31–36, 2017.

[11] D. Miles, "Youth protection: Digital citizenship — principles & new resources," in *2011 2nd Worldwide Cybersecurity Summit*, 2011, pp. 1–3.

[12] "Student access to digital learning resources outside of the classroom." National Centre for Education Statistics. [Online]. Available: https://nces.ed.gov/pubs2017/2017098/index.asp

[13] A. Bizga, "Why should you teach cybersecurity to your kids." Securityboulevard.com. [Online]. Available: https//securityboulevard.com/2020/05/why-should-you-teach-cybersecurity-to-your-kids/

[14] A. V. R. Chandran and S. R. Thangamuthu, “Cyber stalking among higher secondary school students in Kerala,” *Indian J. Educational Tech.*, vol. 2, no. 2, pp. 53–63, 2020.

[15] A. Khan, Z., V. R. Thakur, and Arjun,“Cyber crime awareness among Msw students, school of social work, Mangaluru,” *J. Forensic Sci. Crim. Investig.*, vol. 9, no. 2, pp. 1–7, 2018, doi: 10.19080/jfsci.2018.09.555757.

[16] J. Singh, “To analyze cyber crime awareness of class XII students," *Sch. Res. J. Interdiscip. Stud.,* vol. 1, no. 1, pp. 1326–1330, 2013.

[17] P. Saxena, B. Kotiyal, and R. H. Goudar, “A cyber era approach for building awareness in cyber security for educational system in India,” *Int. J. Inf. Educ. Technol.*, vol. 2, no. 2, pp. 167–170, 2012, doi: 10.7763/ijiet.2012.v2.102.

[18] S. Dhapola, “More kids are online, but Indian parents are finally taking stock: Intel study.” indianexpress.com. Accessed: Jun. 2, 2021. [Online]. Available: https://indianexpress.com/article/technology/tech-news-technology/more-kids-are-online-but-indian-parents-are-finally-taking-stock-intel-study/

[19] A. Shetty, “India ranks third on global cyber bullying list.” FirstPost.com. Accessed: Jun. 5, 2021. [Online]. Available: https://www.firstpost.com/tech/news-analysis/india-ranks-third-on-global-cyber-bullying-list-3602419.html .

[20] K. S. Dhayal, M. Brahmi, S. Agrawal, L. Aldieri, and C. P. Vinci, “A paradigm shift in education systems due to COVID-19: Its social and demographic consequences,” in *Frugal Innov. Social Transitions Digit. Era,* M. N. Tunio and A. B. Memon, Eds. Hershey, PA, USA: IGI Global, 2023, pp. 157–166, doi: 10.4018/978-1-6684-5417-6.ch015.

[21] S. Das, “Growing up in a digital world: Vulnerabilities of children in post-pandemic India.” *LSE Res. Online*. lse.ac.uk. Accessed: Mar. 1, 2023. [Online]. Available: https://blogs.lse.ac.uk/southasia/2021/11/29/growing-up-in-a-digital-world-vulnerabilities-of-children-in-post-pandemic-india/

[22] N. Stanković and V. Ružičić, “Cyber security in education,” in *9th Int. Scientific Conf. Technics Inform. Educ. – TIE 2022*, 2022, pp. 297–301, doi: 10.46793/TIE22.297S.

[23] R. Singh and N. S. Mangat, “Simple random sampling,” in *Elements Surv. Sampling Kluwer Texts Mathematical Sciences*, vol. 15. Springer, Dordrecht, doi: 10.1007/978-94-017-1404-4_3.

[24] Ministry of Electronics and Data Protection, “The digital personal data protection bill, 2022.” Meity.gov.in. Accessed Mar. 3, 2023. [Online]. Available: https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022

[25] A. Berchtold , "Test–retest: Agreement or reliability?" *Methodological Innovations*, vol. 9, pp. 1–7, 2016, doi: 10.1177/2059799116672875.

[26] J. L. Rodgers and W. A. Nicewander, “Thirteen ways to look at the correlation coefficient,” *Am. Stat.*, vol. 42, no. 1, pp. 59–66, 1988, doi: 10.1080/00031305.1988.10475524.

[27] Ministry of Education, “National Education Policy 2020.” Education.gov.in. [Online]. Available: https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English_0.pdf

[28] S. E. Stuart Henderson and A. M. Tania Jarosewich, “Word Cloud.” Betterevaluation.org. [Online]. Available: https://www.betterevaluation.org/en/evaluation-options/wordcloud

About the Authors

Vaishali Chawla has completed Post Graduate degree in Computer Science from Department of Computer Science, University of Delhi, India. Her research interests include Machine Learning, Deep Learning, and Digital Image Processing.

Yatin Kapoor has completed Post Graduate degree in Computer Science from Department of Computer Science, University of Delhi, India. His research interests include Artificial Intelligence, Machine Learning, Deep Learning, Natural Language Processing, and Data Science.

Tanya Chawla has completed Under Graduate degree in Computer Science from Atma Ram Sanatan Dharma College, University of Delhi, India. Her research interests include Machine Learning and Data Science.