EFFECTIVENESS OF CYBER HYGIENE INSTRUCTIONAL MODULE (CIM) ON KNOWLEDGE AND PRACTICE REGARDING CYBER HYGIENE AMONG UNDERGRADUATE STUDENTS.

[1]Ms.Mary Catherin D.E [2]Dr.Prof.P. Genesta Mary Gysel [3]Prof.R.Uma [4]Ms. Aripriya P [5]Ms. Logeshwari R [6]Ms. Madhumidha R [7]Mr. Arun S [8] Mr. Akkash S [9]Ms. Kowsalya S [10]Mr. Kedhuram T

[1]Assistant Professor [2]Principal [3]Vice Principal [4-10]BSc Nursing Officer

[1] Department of Mental Health Nursing.

[1-10]Sabari College of Nursing, Puducherry, India.

Abstract : The evolution of internet, from its origins in the 1960s to the present digital age, has transformed communication. With over 5.35 billion active internet users, individuals are more connected than ever before. However, rapid digitalization has led to rise in cybercrimes such as identity theft, cyberbullying, and data breaches. A major contributing factor to this vulnerability is the lack of awareness regarding cyber hygiene. Cyber hygiene, much like personal hygiene, involves adopting routine practices that ensure online safety and prevent cyber threats. Given the growing digital exposure among undergraduate students and the alarming statistics on cyber risks, there is a pressing need to enhance their knowledge and practices related to cyber hygiene. This study aims to assess the Effectiveness of Cyber hygiene Instructional Module (CIM) on Knowledge and Practice regarding Cyber hygiene among Undergraduate students. Quasi experimental one group pre-test and post-test research design was adopted. Pre-test and post-test were conducted regarding knowledge and practice, CIM intervention was given to the students between pre and post-test. The results revealed that that level of adequate knowledge during pretest was 44.7% and 98.7% during post-test, the level of adequate practice during pretest was 47.3% and during post-test it is 95.3%. It is highly statistically significant showing improvement of Knowledge and practice after attending CIM. The study also shows that students of age 19-20 years had more adequate knowledge on Cyber hygiene, students who used more than 3 gadgets had more adequate knowledge and students those who used more than 5 accounts had more inadequate knowledge on Cyber hygiene. This study clearly emphasizes the importance of structured and targeted cyber hygiene education for students, who are increasingly reliant on digital platforms in both academic and clinical environments. The findings suggest that incorporating such modules in education can play a vital role in reducing vulnerability to cyber threats and ensuring secure handling of digital data. It highlights the potential of such interventions to empower students to serve as responsible digital citizens and educators within their communities. Therefore, regular training programs and updates on cyber hygiene should be prioritized within the curriculum.

Index Terms **- Cyber Hygiene Instructional Module, CIM, Cyber Hygiene, Cyber Hygiene knowledge, Cyber Hygiene Practice**

I. INTRODUCTION

The Internet's origin dates back to the 1960s, when it was conceived as a medium for sharing information among government researchers. The Cold War and the Soviet Union's launch of Sputnik satellite prompted the US Defense Department to develop ARPANET (Advanced Research Projects Agency Network). This precursor to the Internet enabled communication between government and academic institutions. With the adoption of Transfer Control Protocol/Internet Protocol (TCP/IP) in 1983, the Internet officially took shape, facilitating communication between disparate computer networks.[1]

The number of active internet users worldwide was estimated to be 4.57 billion as of July 2020, comprising 59 % of the entire world population.[2] As the web has become more accessible and popular, smartphones utilizing new technologies such as 4G, 5G and very soon 6G, became the vital channel for internet access worldwide as mobile internet users account for 91 % of total internet customers. This reflects how the internet and web have ended up being relatively vital to individuals, professionals, and companies across the globe. Today, people, experts and companies are making use of social media on an everyday basis, sharing details, or promoting their company or brands. [3-4]

During the pandemic, strict social distancing measures prevented India's 1.3 billion-strong population from engaging with others in-person, leading more people to turn to digital channels. [5] Social media has blurred the lines between the virtual and the real world, thereby transforming the world into a global village, with distance no longer a barrier today. More than 66 percent of all the global

population uses the internet, with the latest data from Data Reportal putting the global user total at 5.35 billion. Additionally, the internet users have risen by 1.8 percent over the past 12 months, owing to the new 97 million users since the start of 2023.[6]

According to National Cyber Crime Reporting Portal cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime".[7] What distinguishes cybercrime from traditional criminal activity is obviously, the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous.[8]

Cybercrime on whole includes child pornography/ child sexually abusive material (CSAM), cyber bullying, cyber stalking, cyber grooming, online Job Fraud, online sextortion, vishing, sexting, smishing, SIM Swap Scam, debit/credit Card Fraud, impersonation and identity theft, phishing, spamming, ransomware, virus, worms & trojans, data breach, denial of services, website defacement, cyber-squatting, pharming, cryptojacking, online drug trafficking and espionage.[7]

A major contributing factor to the rise of cybercrime in India is the lack of awareness and education about cybersecurity. Many individuals and organizations do not possess the necessary knowledge to identify potential threats or take appropriate preventive measures. This knowledge gap makes them easy targets for cybercriminals.[9]

Cyber hygiene is about training people to form good habits around cybersecurity so that they can stay ahead of cyber threats and online security issues. Cyber hygiene is sometimes compared to personal hygiene in that both are precautionary processes carried out regularly to ensure health and wellbeing. Practiced regularly, cyber hygiene helps to keep data safe and secure. Building a routine around cyber hygiene will help prevent cybercriminals from causing security breaches or stealing personal information. It will also help people to be up to date with software and operating systems. As a concept, cyber hygiene has increased in relevance since the Covid-19 pandemic, as more people around the world working remotely led to a rise in cybercrimes.[10]

NEED FOR THE STUDY

Nearly 5.35 billion people currently use social media worldwide, more than double from 2.07 billion in 2015. The average social media user engages with an average of 6.7 various social media platforms and 63.7% of the global population in the world uses social media. Globally, the average time a person spends on social media a day is 2 hours 20 minutes. Facebook is the leading social network with 3.07 billion monthly active users, followed by YouTube (2.5 billion), WhatsApp (2 billion), Instagram (2 billion), and TikTok (1.58 billion). 94.9% of 5.45 billion global internet users and 91% of 5.68 billion mobile phone users are on social media. Out of 5.45 billion internet users, 94.9% are active users. A study of 53 countries with internet users aged 16+ shows Japan had the lowest average number of social platforms used at 3.5, comparably Brazil had the highest with 8.0 per internet user.[11]

India ranks second with just under half of its population 49.15 % using the internet that accounts to 692 million people. [12] As the world is advancing in the realm of digitalization, the threat of cyber-attacks has also grown and India is no exception to it. In October, 2023, Resecurity, a US company, informed the world about the availability of Indian's personal data on the dark web. It would have been easy to ignore this amid the deluge of bad news filling the news feeds but for the size and sensitivity of data. The seller of the data set was providing verifiable, sensitive information of 55% of the Indian population roughly around 815 million (81.5 crore) citizens. The data included personally identifiable information like name, phone number, Aadhaar number, passport number and address.[13]

In October 2019, there was an attempted cyber-attack on the Kudankulam Nuclear power plant. There was malware attack on the City Union Bank's SWIFT system which led to unauthorised transactions worth USD 2 million in March 2020. In May 2021, the personally identifiable information (PII) and test results of 190,000 candidates for the 2020 Common Admission Test (CAT), used to select applicants to the IIMs, were leaked and put up for sale on a cybercrime forum. In December 2020, a global cyber-attack on Solar-Winds, a US-based software company that provides network management tools, affected several Indian organizations, including the National Informatics Centre (NIC), the Ministry of Electronics and Information Technology (MeITY), and Bharat Heavy Electricals Limited (BHEL).[13]

According to a data given by the government in parliament, India saw approximately 1.16 million cyber-attacks in 2020, with a median of 3,137 cyber security incidents recorded every day of the year. India is placed at third position among the first 20 countries which are affected by cybercrime, according to the FBI's Internet Crime Report.[14]

The Indian Computer Emergency Response Team (CERT-In) has "reported 49,455 cybersecurity incidents in 2015, 50,362 in 2016, 53,117 in 2017, 2,08,456 in 2018, 394,499 in 2019 and 696,938 cybersecurity incidents during the year 2020 (till August), the MeITY said while responding to an unstarred question in the Lok Sabha regarding cyber-attacks on Indian citizens and India-based commercial and legal entities.[15]

According to NCRB data, the number of cybercrimes grew by 63.48% from 2018 to 2019 with over 33% of children experiencing online bullying, India has the highest prevalence of online harassment.[16] Internet users in India continued to fall victims to cyber-attacks with nearly a quarter of users, 20%, falling victims to cyber threats in the first quarter of 2024. While nearly 22.9% users were attacked by web-borne threats, 20.1% users were found to be vulnerable to local threats during the same period.[17]

According to study conducted by Child Rights and You (CRY), a non-governmental organization Around 9.2% of 630 adolescents surveyed in Delhi-National Capital Region had experienced cyberbullying and half of them had not reported it to teachers, guardians or the social media companies concerned and one in four adolescents also reported seeing a morphed image or video of themselves, and 50% of these were not reported to the police.[18]

The NCRB report reveals a total of 1,823 cases of cybercrime against children in 2022, up from 1,376 the previous year (2021). These crimes include 1,171 cases of cyber pornography or the dissemination of inappropriate content, 158 cases of cyber stalking and bullying and 416 other cyber related offenses.[19] According to a report released by DQ Institute at the Global Cybersecurity Forum in Riyadh on November 10, 2024 almost three in four (73%) children and adolescents aged 8-18 around the world experienced at least one cyber risk in the 12 months to September 2022. This report also revealed that 50% of children and adolescents across the surveyed countries are

affected by cyber-bullying, 40% experience cyber threats, 25% are exposed to violent and sexual content, 16% are at risk for a gaming disorder, 8% are at risk for social media disorder and 40% of adolescents (aged 13-18) experience unwanted sexual contact. This was the final conclusion of the survey which was taken across 100 countries including 3,30,000 children and adolescent using Child Online Safety Index.[20]

In India, smartphone use at the age of 10 to 14 is at 83 per cent, which is significantly 7 per cent above the international average of 76 per cent. This leads to high exposure to online risks as there is a substantial security gap between parents and children. Additionally, while the concern is relatively low among parents, 22 per cent of Indian children experienced cyberbullying at some time which is notably 5 per cent higher than the global average of 17 per cent.[21]

Statement of the problem:

A study to Assess the Effectiveness of Cyber hygiene Instructional Module (CIM) on Knowledge and Practice regarding Cyber hygiene among Undergraduate students.

Objectives of the study:

- To assess the level of knowledge and practice regarding cyber hygiene among Undergraduate students
- To evaluate the effectiveness of CIM on knowledge and practice regarding cyber hygiene among Undergraduate students.
- To associate the level of knowledge and practice regarding cyber hygiene among Undergraduate students with selected demographic variables.

II. METHODOLOGY:

The study adopted a quantitative research approach to systematically measure and evaluate the effectiveness of the Cyber Hygiene Instructional Module (CIM). This approach enabled the collection of numerical data on student's knowledge and practice regarding cyber hygiene both before and after the intervention, facilitating objective analysis and comparison of outcomes.

A quasi-experimental one-group pre-test and post-test design was employed to assess the impact of the instructional module. This design involved administering a structured questionnaire to the same group of undergraduate students prior to the intervention, followed by implementation of the CIM, and then reassessing the same group using the same tool after a five-day interval. This design was chosen as it allows for evaluation of the effectiveness of the intervention without the use of a control group. In this study the population are undergraduate students and who are in the age category of 17 to 24 years old and target population is B.Sc Nursing students studying in Sabari college of Nursing.

Independent variable:

The independent variable in this study is the Cyber Hygiene Instructional Module (CIM), a structured educational intervention developed to enhance knowledge and practice related to cyber hygiene among undergraduate students. The module comprises eight comprehensive components, each designed to address key aspects of safe digital behavior:

1. *Cyber Threats and Risks* – Introduction to common cyber threats such as malware, phishing, ransomware, and social engineering tactics, along with real-world examples relevant to students.
2. *Password Management* – Guidance on creating strong, unique passwords and the importance of multi-factor authentication to secure online accounts.
3. *Online Safety* – Best practices for safe browsing, identifying secure websites, avoiding suspicious downloads, and protecting personal information while using the internet.
4. *Data Protection* – Emphasis on securing sensitive data, understanding data privacy rights, and handling digital files responsibly.
5. *Social Media and Online Presence* – Raising awareness about the digital footprint, privacy settings, and the implications of sharing personal information on social platforms.
6. *Email and Messaging Security* – Recognizing and handling spam, phishing emails, suspicious links, and the importance of encrypted messaging.
7. *Device and Network Security* – Basic principles of securing personal devices through antivirus software, regular updates, and safe use of public Wi-Fi.
8. *Incident Response* – Steps to take in case of a cyber incident, including reporting, mitigation, and recovery strategies.

Dependent variable:

The dependent variable of the study are Knowledge and Practice regarding Cyber Hygiene among undergraduate students.

Sampling technique:

A convenience sampling technique was used to select participants for the study.

Sampling size:

The Sample size for this study is 150 students

Sampling criteria:

Inclusion criteria:

- Students studying B.Sc Nursing at Sabari college of Nursing
- Students who use digital gadgets.
- Who were available at the time of data collection.

Exclusion criteria:

- Students who were not willing to participate in the study

Description of tool:

A structured questionnaire was used to assess the knowledge and practice regarding cyber hygiene The tool was developed in alignment with the content of the Cyber Hygiene Instructional Module (CIM), expert validation, and literature review. It comprised two main parts:

Socio-Demographic Profile

This section consisted of 13 items to gather personal and background information of the students, including age, gender, year of study, area of residence, type of digital devices used, internet usage patterns, social media presence, and parental education. This data supported the analysis of possible associations with knowledge and practice levels.

Knowledge and Practice Questionnaire

Knowledge Section: Included 35 multiple-choice questions covering various dimensions of cyber hygiene, such as cyber threats, online safety, data protection, and device security. Each correct answer was scored as 1, with the total score ranging from 0 to 35.

Practice Section: Comprised 15 items to assess day-to-day cyber hygiene practice.

The same tool was administered during both the pre-test and post-test phases to evaluate changes in knowledge and practice following the intervention.

Ethical consideration

Prior to data collection, ethical approval was obtained from the Institutional Ethical Committee. The purpose, benefits, and procedures of the study were clearly explained to all students, and informed written consent was obtained.

Data collection procedure:

The data collection process was carried out in three distinct phases.

1. Permission for the Study Setting
2. Pre-Test Assessment and Intervention (Cyber Hygiene Instructional Module)
3. Post-Test Assessment

DATA ANALYSIS

Descriptive Statistics:

Frequency and Percentage: These were used to describe the socio-demographic characteristics of the students.

Inferential Statistics:

McNemar Test: This test was applied to evaluate the effectiveness of the Cyber Hygiene Instructional Module (CIM). The McNemar test compares the pre-test and post-test results of the same students to determine whether there was a statistically significant change in their knowledge and practices regarding cyber hygiene. It is especially useful when dealing with paired nominal data (before and after measures).

Chi-Square Test: The Chi-square test was used to explore any associations between socio-demographic variables (such as age, gender, year of study, and digital device usage) and the level of knowledge and practice of cyber hygiene. This test helps identify if specific demographic factors influence participant's understanding and practice related to cyber hygiene.

IV. RESULTS

In regards to age 44(29%) years were 17-18, 99(66%) were 19-20 years, 6(4%) were 21-22 years and 1 was 23-24 years. Among the 150 participants 38 (25%) were male and 112 (75%) were female. When taking account the education of the father 39(26%) of student's fathers have done Primary schooling, 47(31.4%) of student's fathers have done High schooling, 28(18.6%) of student's fathers have done higher secondary, 23(15.4%) of student's fathers are undergraduates and 13(8.6%) of student's fathers are Post graduate. When taking account the education of the mother 40(26.6%) of student's mothers have done Primary schooling, 40(26.6%) of student's mothers have done High schooling, 34(22.7%) of student's mothers have done higher secondary, 20(13.4%) of student's mothers are undergraduates and 16(10.7%) of student's mothers are Post graduate. Regarding the number of gadgets used 73(48.6%) of students use only 1 gadget, 36 (24%) of students use 2 gadgets, 18(12%) of students use 3 gadgets and 23(15.4%) of students use more than 3 gadgets. Regarding number of social media account 111 (74%) of students have less than 3 accounts, 27(18%) of students have 3- 5 accounts and 12(8%) of students have more than 5 accounts. Regarding the average screen time in a day 78(52%) of students have screen time less than 4 hours, 58(39%) of students have screen time 5-7 hours, 13(8.5%) of students have screen time 8-10 hours and 1 (0.5%) student has screen time more than 10 hours. Considering years of social media usage 78(52%) of students use social media for less than 3 years, 36(24%) of students use social media for 3-5 years and 36(24%) of students use social media for more than 5 years. Regarding the source of internet 128(85.3%) of students use mobile data, 14(9.4%) of students use private Wi-Fi connection and 8(5.3%) of students use free and public Wi-Fi connection. Regarding own mobile phone 130(86.4%) of students have their own mobile phone and 20(13.4%) do not their own mobile phone.

Table 1 shows that level of adequate knowledge during pre-test was 44.7% and 98.7% during post-test with p value 0.001. The level of adequate practice during pre-test was 47.3 % and during post-test it is 95.3 % with p value 0.001. It is highly statistically significant showing improvement of Knowledge and practice after attending Cyber-Hygiene Instructional module. (Figure 1.1)

Table 1 : Pre-test and Post-test level of Knowledge and Practice.

S.no	Parameter	Outcome	Pre-test		Post-test		P Value
			Frequency (N)	Percentage (%)	Frequency (N)	Percentage (%)	
1	**Knowledge**	Inadequate Knowledge (1-13)	83	55.3	2	1.3	**0.001***
		Adequate Knowledge (14-35)	67	44.7	148	98.7	
2	**Practice**	Inadequate Practice (1-7)	79	52.7	7	4.7	**0.001***
		Adequate Practice (8-15)	71	47.3	143	95.3	

***significant at P<0.05**

The result also revealed few socio demographic variables were associated with level of knowledge. The students of age 19-20 years had more adequate knowledge on Cyber hygiene with p value 0.024, students who used more than 3 gadgets had more adequate knowledge with p value 0.020 and students those who used more than 5 accounts had more inadequate knowledge on Cyber hygiene with p value 0.003. At the same time no association was found between socio demographic variables and level of practice.

IV. DISCUSSION

The findings of the study have major implication in the field of education, administration, research and services.

Research: The present study provides a strong foundation for future research to explore the impact of cyber hygiene not only among students but also among nursing professionals working in clinical settings. Research can be extended to assess the role of cyber hygiene in hospital information systems (HIS), focusing on the prevention of data breaches and ensuring patient information confidentiality. Further research can also be directed towards evaluating the effectiveness of various cyber security training modules tailored for nurses handling digital records and electronic health information systems.

Administration: Administrators may also collaborate with cyber experts to create guidelines for safe internet usage within the institutional environment. From an administrative perspective, the study highlights the responsibility of nursing administrators in establishing policies and protocols for safe cyber practices within healthcare institutions. Administrators should ensure that all nurses working with HIS and electronic medical records receive adequate training on cyber hygiene practices such as secure login methods, data encryption, regular password updates, and reporting suspicious online activities. Nursing administrators can also collaborate with IT departments to develop institutional guidelines to prevent cyber threats and ensure safe handling of patient data. ***Practice:*** This implies that nurses, being active users of technology in both personal and professional domains, should be equipped with appropriate knowledge and skills to practice cyber hygiene effectively. Nurses can play a vital role in creating awareness among patients, families, and the community regarding safe internet practices. Nursing professionals should incorporate cyber hygiene practices in their routine to prevent cyber-related risks and to promote safe handling of digital information, especially in healthcare settings where patient data confidentiality is crucial. ***Education:*** The results of the study strongly indicate the need to incorporate cyber hygiene and cyber safety education into the nursing curriculum. Nurse educators should take initiatives to design suitable instructional modules, workshops, or simulation-based learning methods to enhance the knowledge and practice regarding cyber hygiene among nursing students. It is essential to update students regarding recent advancements in technology, cyber laws, and online safety guidelines to prepare them to handle cyber-related challenges effectively in both academic and clinical settings. Incorporating real-time case scenarios, cyber incident handling strategies, and role plays can enhance students' skills in managing cyber safety effectively. Moreover, educational institutions should promote a culture of responsible digital behavior and emphasize the legal and ethical aspects of cyber security in nursing practice.

RECOMMENDATION

Based on the findings of the study the following recommendation has been made for the further study.

1. A comparative study may also be undertaken between nursing students and students from other professional courses such as medical, engineering, or arts and science streams to assess their level of knowledge and practice regarding cyber hygiene.
2. A qualitative research approach may also be used to explore the lived experiences, challenges, and perceptions of students regarding maintaining cyber hygiene practices in their day-to-day life.
3. A longitudinal study can be carried out to assess the long-term retention of knowledge and practice regarding cyber hygiene after the implementation of instructional modules or educational interventions.
4. Future research can focus on the development and validation of standardized tools such as Cyber Hygiene Practice Scale or Cyber Awareness Assessment Tool for use among various populations like school students, college students, and working professionals.
5. Interventional studies can be planned focusing on the role of mobile applications, e-learning platforms, and social media campaigns in promoting cyber hygiene practices among young adults.
6. Mixed-method research may also be carried out to explore the barriers and facilitators influencing cyber hygiene practices among students, which will help in developing more customized and effective educational interventions in the future.

V. CONCLUSION:

This study aimed to assess the effectiveness of Cyber hygiene Instructional Module (CIM) on cyber hygiene among undergraduate students. A significant improvement was observed from pre-test to post-test in both knowledge and practice levels, indicating the positive impact of the educational intervention. The post-test findings revealed that a vast majority of students demonstrated adequate knowledge and practice, which was statistically significant (p=0.001). This clearly emphasizes the importance of structured and targeted cyber hygiene education for nursing students, who are increasingly reliant on digital platforms in both academic and clinical environments. The findings suggest that incorporating such modules in nursing education can play a vital role in reducing vulnerability to cyber threats and ensuring secure handling of digital data, especially within healthcare settings. Furthermore, it highlights the potential of such interventions to empower nursing students to serve as responsible digital citizens and educators within their communities. Therefore, regular training programs and updates on cyber hygiene should be prioritized within the nursing curriculum to build a cyber-aware future healthcare workforce.

Funding: This was a self funding Project.

Competing interests: The authors declare that we have no competing interests.

Acknowledgements: Nil

REFERENCES

1. GeeksforGeeks. History of Internet. Available from: https://www.geeksforgeeks.org/history-of-internet/

2. Statista. Worldwide digital population as of July 2020. Statista; 2020 [cited 2025 Apr 17]. Available from: https://www.statista.com/statistics/617136/digital population-worldwide/

3. Roser M, Ritchie H, Ortiz-Ospina E. The internet's history has just begun. Our World in Data; 2015 [cited 2025 Apr 17]. Available from: https://ourworldindata.org/internet

4. Miniwatts Marketing Group. Internetworldstats . Internetworldstats; 2020 [cited 2025 Apr 17]. Available from: https://www.internetworldstats.com/stats.htm

5. OOSGA. Social Media Statistics India. Available from: https://oosga.com/social-media/ind/

6. Indian Express. Top 10 most popular social media platforms as of 2024. Indian Express; 2024 [cited 2025 Apr 17]. Available from: https://indianexpress.com/article/trending/top-10-listing/top-10-most-popular-socialmedia-platforms-as-of-2024-9526794/

7. Government of India. Cybercrime. Cybercrime.gov.in. Available from: https://cybercrime.gov.in/Webform/CrimeCatDes.aspx

8. Encyclopaedia Britannica. Cybercrime. Available from: https://www.britannica.com/topic/cybercrime

9. Hashmi A. The rise of cybercrime in India: reasons, impacts, and safety measures. LinkedIn; 2022 [cited 2025 Apr 17]. Available from: https://www.linkedin.com/pulse/rise-cybercrime-india-reasons-impacts-safetymeasures-adil-hashmi/

10. Kaspersky. Cyber Hygiene Habits. Kaspersky. Available from: https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

11. Backlinko. Social Media Users. Backlinko; 2022 [cited 2025 Apr 17]. Available from: https://backlinko.com/social-media-users

12. Times of India. 10 countries with the highest number of internet users. Times of India; 2024 [cited 2025 Apr 17]. Available from: https://timesofindia.indiatimes.com/technology/tech-news/10-countries-with-thehighest-number-of-internet-users/photostory/111014666.cms

13. Drishti IAS. India's cybersecurity challenge: threats and strategies. Drishti IAS; 2024 [cited 2025 Apr 17]. Available from: https://www.drishtiias.com/dailyupdates/daily-news-editorials/india-s-cybersecurity-challenge-threats-and-strategies

14. International Journal of Advanced Legal Research. The current state of cyber security in India. IJALR; 2024 [cited 2025 Apr 17]. Available from: https://ijalr.in/the-current-state-of-cyber-security-in-india/

15. Inc42. 3.94 lakhs and counting: How cyberattacks are a worry for Digital India . Inc42; 2024 [cited 2025 Apr 17]. Available from: https://inc42.com/buzz/3-94lakhs-and-counting-how-cyberattacks-are-a-worry-for-digital-india/

16. 2024 ResearchGate. The growing threat of cyberbullying in India . ResearchGate; [cited

2025Apr17].Availablefrom:https://www.researchgate.net/publication/372724976_The_Growing_Threat_of_Cyberbullying_in_India

17. The Hindu. 20 Indian users fell victim to cyber threats in the first quarter of 2024, finds study. The Hindu; 2024 [cited 2025 Apr 17]. Available from: https://www.thehindu.com/sci-tech/technology/20-indian-users-fell-victim-to-cyberthreats-in-the-first-quarter-of-2024-finds-study/article68196110.ece

18. IndiaSpend. 1 in 10 Indian adolescents faces cyberbullying; half don't report, study. IndiaSpend; 2024 [cited 2025 Apr 17]. Available from: https://www.indiaspend.com/1-in-10-indian-adolescents-faces-cyberbullying-half-dont-report-study/

19. Times of India. Child cybercrime surges 32%, reveals NCRB data underlining vulnerability to online risks . Times of India; 2024 [cited 2025 Apr 17]. Available from: https://timesofindia.indiatimes.com/india/child-cyber-crime-surges-32-revealsncrb-data-underlining-vulnerability-to-online-risks/articleshow/107168056.cms

20. DQ Institute. Three in four children worldwide experienced at least one cyber risk in 2022. DQ Institute; 2022 [cited 2025 Apr 17]. Available from: https://www.dqinstitute.org/news-post/three-in-four-children-worldwide-experiencedat-least-one-cyber-risk-in-2022/

21. Indian Express. Indian children have the highest online risk exposure: McAfee's 2022 connected family . Indian Express; 2022 [cited 2025 Apr 17]. Available from: https://indianexpress.com/article/technology/tech-newstechnology/indian-children-have-the-highest-online-risk-exposuremcafees-2022connected-family-7915324/