



THE ROLE OF EDUCATION IN ENHANCING CYBERSECURITY AWARENESS AND DIGITAL SAFETY AMONG ADOLESCENT GIRLS AGED 13–19

Prof. Dr. Saraswati Raju Iyer¹, Vishwaja Rangannagari², Thiruveedula Seshu Babu³

¹Professor, Chairperson, P.G. BoS in Sociology & Social Work, Department of Sociology & Social Work, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.

²Ph.D. Research Scholar in Sociology, Department of Sociology & Social Work, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.

³UGC NET SRF, Ph.D. Research Scholar in Social Work, Department of Sociology & Social Work, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.

Article DOI: <https://doi.org/10.36713/epra31922>

DOI No: 10.36713/epra31922

ABSTRACT

Education plays a vital role in empowering adolescent girls to understand and respond effectively to cyber threats in an increasingly digital society. This study examines the implementation of cybersecurity education in schools, girls' perceptions of online safety, and the role of educators in promoting cybersecurity awareness. The study adopts a descriptive research design in Guntur district, Andhra Pradesh, using purposive sampling to select 90 female students and 90 teachers. Primary data were collected through structured interview schedules, while secondary data were obtained from journals, books, reports, and news articles. The collected data were analyzed using percentages, graphs, and pie charts.

The findings reveal that all student respondents use the internet daily, with 63% reporting six to ten hours of daily usage. Although 67% expressed some confidence in navigating online threats, 30% reported that they or their acquaintances had experienced cyberbullying or online harassment. A significant gap was identified in formal cybersecurity education, as all student respondents reported that their schools did not conduct specialized cybersecurity classes or programmes. Furthermore, 70% considered school-based online safety education extremely important, and all respondents supported a more active role for teachers in promoting cybersecurity awareness. Teachers also recognized the importance of cybersecurity education and expressed support for targeted educational initiatives.

The study highlights the need to integrate structured cybersecurity education into school curricula, provide specialized training for teachers, strengthen parent–teacher collaboration, and incorporate practical exercises, real-life case studies, and expert-led workshops. It concludes that comprehensive and gender-sensitive cybersecurity education can strengthen digital literacy, improve online safety practices, and empower adolescent girls to navigate digital spaces more confidently and responsibly.

KEYWORDS: Cybersecurity education, adolescent girls, cyber threats, online safety, cyberbullying, digital empowerment.

INTRODUCTION

The widespread impact of the internet in the modern digital age emphasizes how important it is to teach young people how to navigate the internet safely. The internet offers a plethora of benefits, but it also exposes students to concerns such as cyberbullying, privacy violations, and security vulnerabilities.

In our current digitally connected world, young people, particularly girls between 13–20 experience a host of cyber threats online from inappropriate content and cyberbullying to privacy invasion and identity theft. The dangerous threats on the online frontier are too many, but as the girls move across the landscapes of the internet, one cannot forget the central part that education has to play in empowering girls to protect themselves in the virtual world. Education is key to ensuring girls are equipped with the knowledge, skills and confidence to navigate the online world safely and responsibly.

REVIEW OF LITERATURE

Education plays a crucial role in empowering girls to navigate cyber threats effectively. By providing girls with the necessary skills and knowledge, education can enable them to protect themselves from online dangers and make informed decisions while engaging with the digital world (Sulaiman. NS.2023).

Studies have shown that promoting cyber hygiene practices among young girls can enhance their cautiousness and behaviour, leading to safer internet usage and protection against cyber-attacks (Kanchana, Dr & Y, Ms & M, Ms & J, Ms. 2022).

Additionally, tailored cyber education initiatives have been identified as essential in helping girls understand specific cyber threats faced by different sectors, such as small and medium enterprises, and the potential consequences of cyber-attacks on production processes (Akinola.O. 2023).



Furthermore, the development of cyber security skills through training programs can empower teachers to support students in implementing cyber security tools and techniques to reduce risks (Kyva, V., Zastelo, O., & Nakonechnyi, O. 2022).

Educators can play a significant role in educating learners about cyber safety, thereby empowering them to handle cyber incidents effectively (Sonhera, N., Kritzing, E., & Looock, M. 2021).

Moreover, promoting safe and responsible internet use among young people is crucial for enhancing their cyber-wellness and developing digital resilience (Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. 2021).

By integrating frameworks that focus on technology readiness and organizational security adoption, organizations can enhance their cyber security readiness and ultimately benefit from improved performance (Berlilana, Tim Noparumpa, Athapol Ruangjanases, Taqwa Hariguna, and Sarmini. 2021). Overall, education serves as a cornerstone in empowering girls to navigate cyber threats by equipping them with the necessary knowledge, skills, and resilience to protect themselves in an increasingly digital world.

NEED FOR THE STUDY

There is a need for this study as teenagers are more vulnerable to cyber-crimes if there is lack of proper guidance. The growing use of smartphones and the internet has increased women's and girls' susceptibility to cybercriminals (Balabantaray, Subhra & Mishra, Mausumi & Pani, Upananda, 2023). This guidance should be mostly provided by schools as a part of their curriculum. Andhra Pradesh is standing in fifth position in cyber-crimes according to latest published report by National Crime Records Bureau (NCRB) (Crime in India, NCRB, 2022). There has been an enormous increase in cases of crimes against women and girls notably between the ages of 18-30 years old. One of the main reasons for this is lack of awareness and education and rapid technological advancements.

RESEARCH OBJECTIVES

- To assess the implementation of cybersecurity education in schools.
- To explore the perceptions of girls towards cybersecurity and online safety.
- To analyze the role of educators in promoting cybersecurity awareness and empowering girls to navigate cyber threats.

METHODOLOGY

The study is descriptive in nature. The Guntur district of Andhra Pradesh is the study area since it was found to have the second-highest number of cybercrime instances reported there (The Hindu, 2023). A total number of sample respondents of 90 female students and 90 teachers are identified using purposive sampling method. In order to study the above-mentioned research objectives both primary data and secondary data is collected. Primary data is collected by using a structured interview schedule both for students and teachers and secondary data is collected from sources like journals, books, reports, news articles. Interpretation of data is done using percentages, graphs and pie charts.

DATA INTERPRETATION - FEMALE STUDENTS

I. Demographic Profile

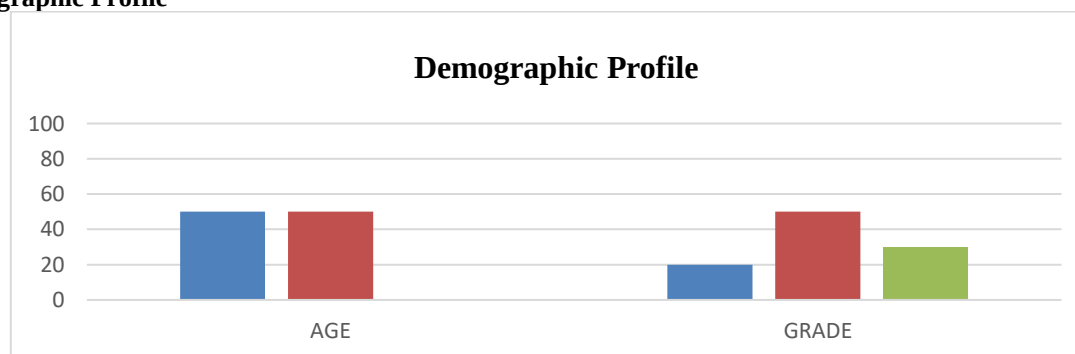


Figure 1.1

Figure 1.1 depicts that half of the respondents belong to the age group of 15-16 years while the other half belong to 17-18 years. Half of the respondents (50%) belong to 11th grade, while 30% belong to 12th class and 20% belong to 10th grade.



II. Internet usage

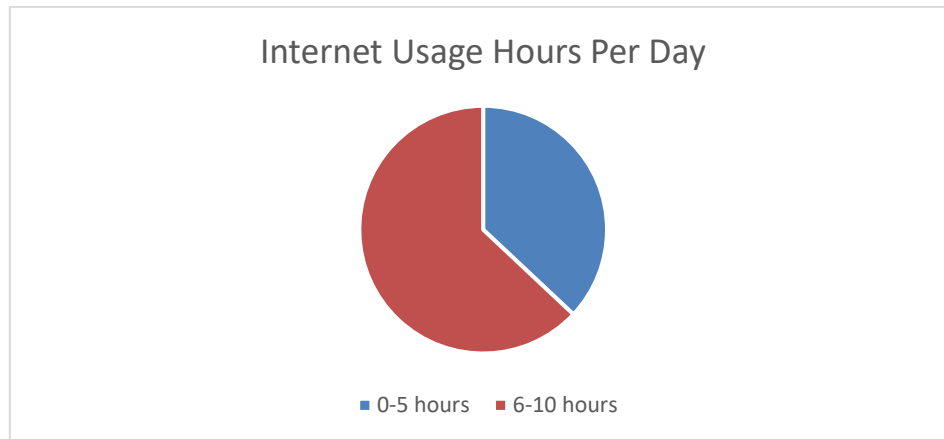


Figure 1.2

In figure 1.2 Cent percent of the respondents have said they use internet daily mostly for their studies and to maintain contacts with friends and family. 37% of the respondents have said that they use internet in between 0-5 hours and 63% have said that they use internet in between 6-10 hours daily.

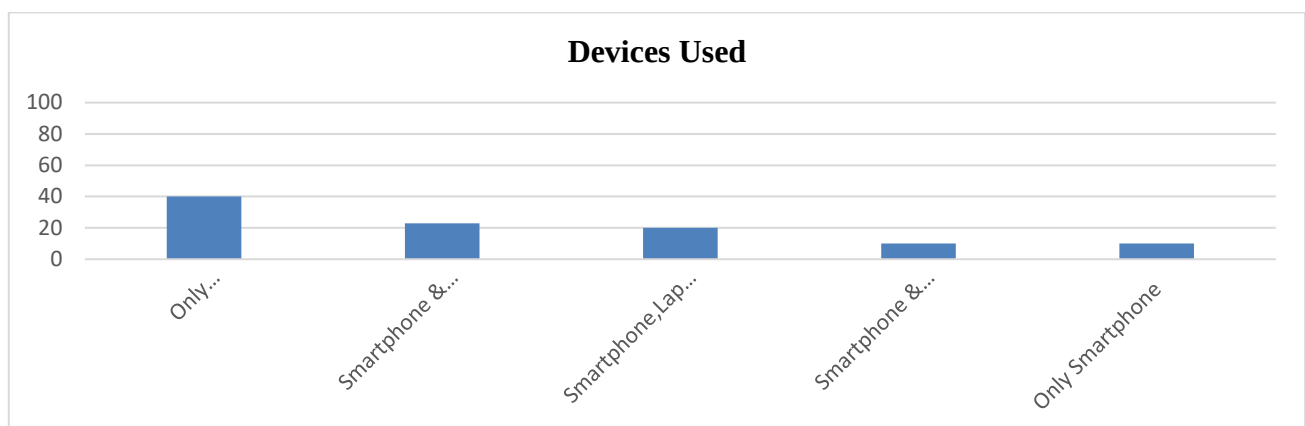


Figure 1.3

In figure 1.3 majority of the respondents (40%) have said they use Laptop/Computer for using internet. 23% have said that they use both smartphone and tablet. 20% have responded that they use all three devices (Smartphone, Laptop/Computer, Tablet). 10% have said that they use both Smartphone & Laptop/Computer. 7% have said that they use only Smartphone for using internet.

III. Social Media usage

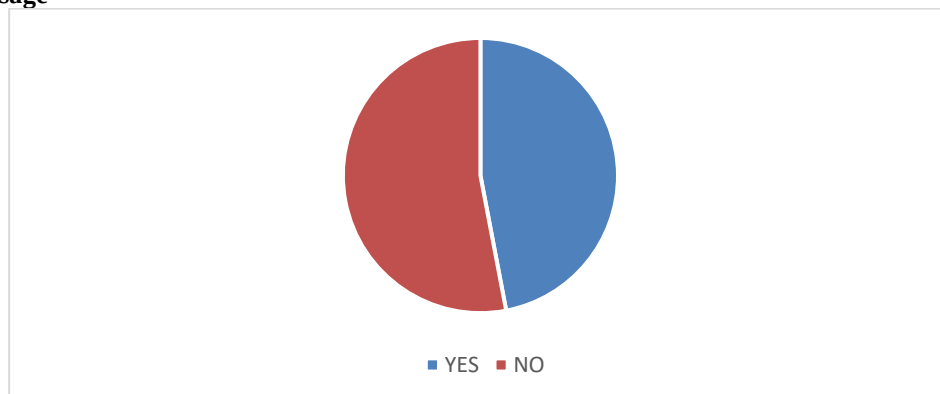


Figure 1.4

This figure shows that majority of the respondents (53%) don't have a social media account and 47% have a social media account.

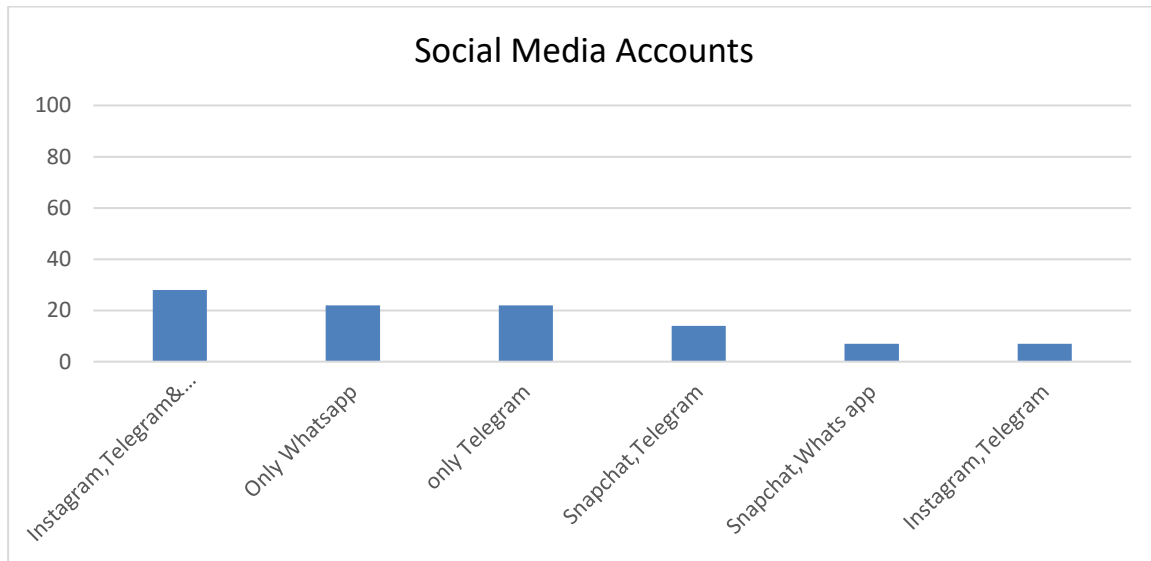


Figure 1.5

Out of the 47% of the respondents who use social media, 28% use Instagram, Telegram and WhatsApp. An equal proportion of the respondents use only Telegram (22%) and only WhatsApp (22%). 14% of them use Snapchat and telegram together. Both snapchat plus WhatsApp is used by 7% of the respondents and another 7% use Instagram plus telegram.

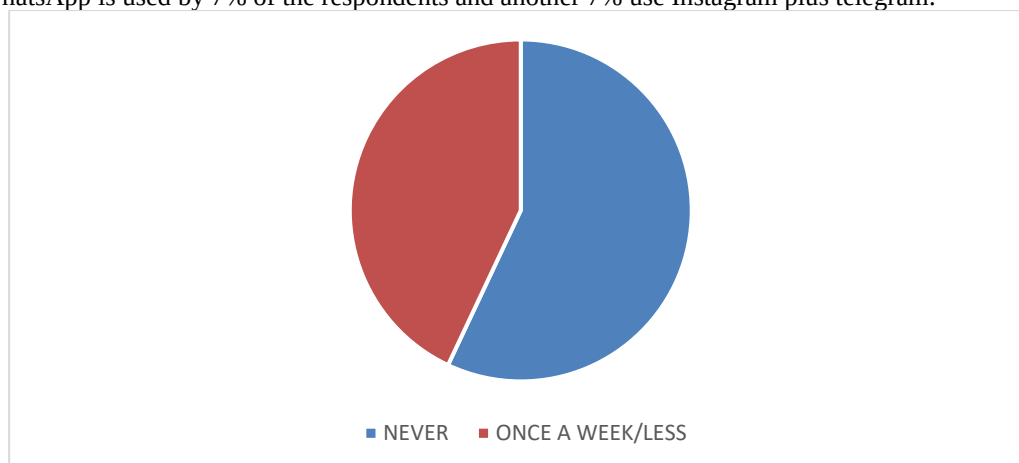


Figure 1.6

More than half of the respondents (57%) have said that they never post content on social media and 43% said that they post content once a week or less.

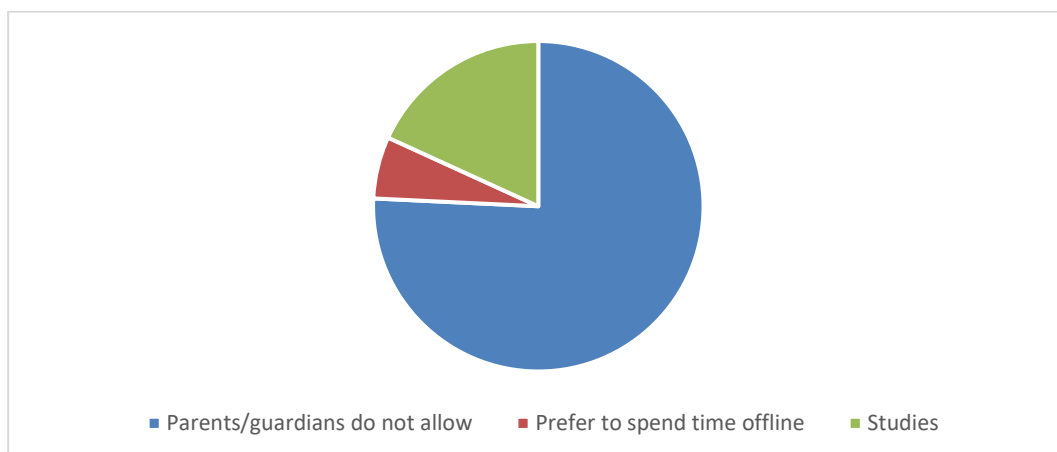


Figure 1.7



Out of the 53% of the respondents, a vast majority of the respondents have said that (75%) they are not using social media account because of the restrictions placed by their parents/guardians. 19% of them don't use because they prefer to spend time offline and 6% of them don't use to concentrate on studies.

IV. Perceptions of Online Safety and Cybersecurity

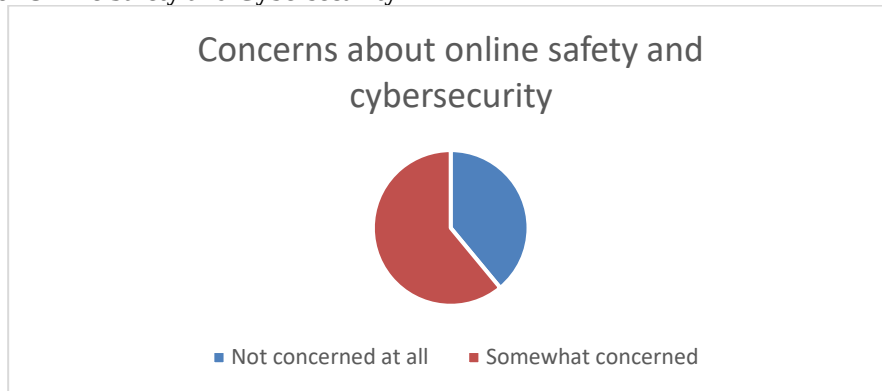


Figure 1.8

More than half of the respondents (63%) are somewhat concerned about online safety and cybersecurity and 37% are not concerned about online safety and cybersecurity.

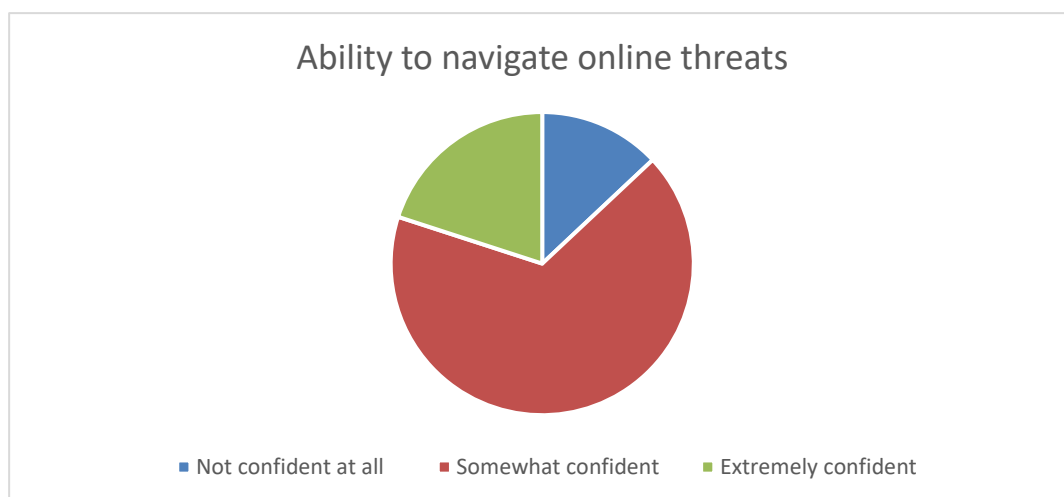


Figure 1.9

Majority of the respondents have said that (67%) they are somewhat confident in their ability to navigate online threats and stay safe on the internet, while 20% said that they are extremely confident and 13% of them said that they are not confident at all in their ability to navigate online threats and stay safe on the internet.

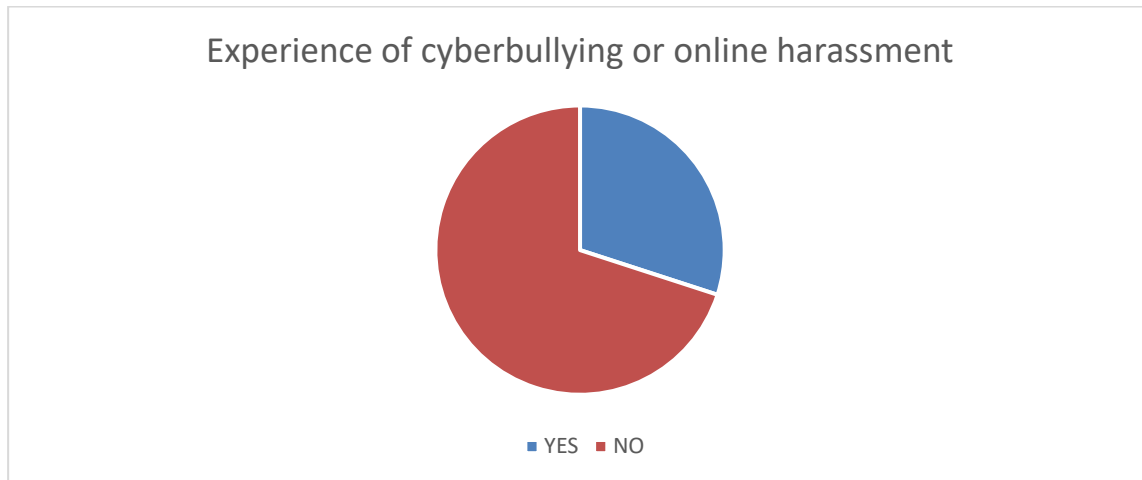


Figure 1.10

Majority of the respondents (70%) have said that they or their acquaintances don't have any experience of cyberbullying or online harassment and 30% have said that themselves or their acquaintances have any experience of cyberbullying or online harassment. All the respondents have said that there is no negative influence or pressure by their peers on their online behavior and attitudes towards cybersecurity.

V. Experience with Educational Initiatives

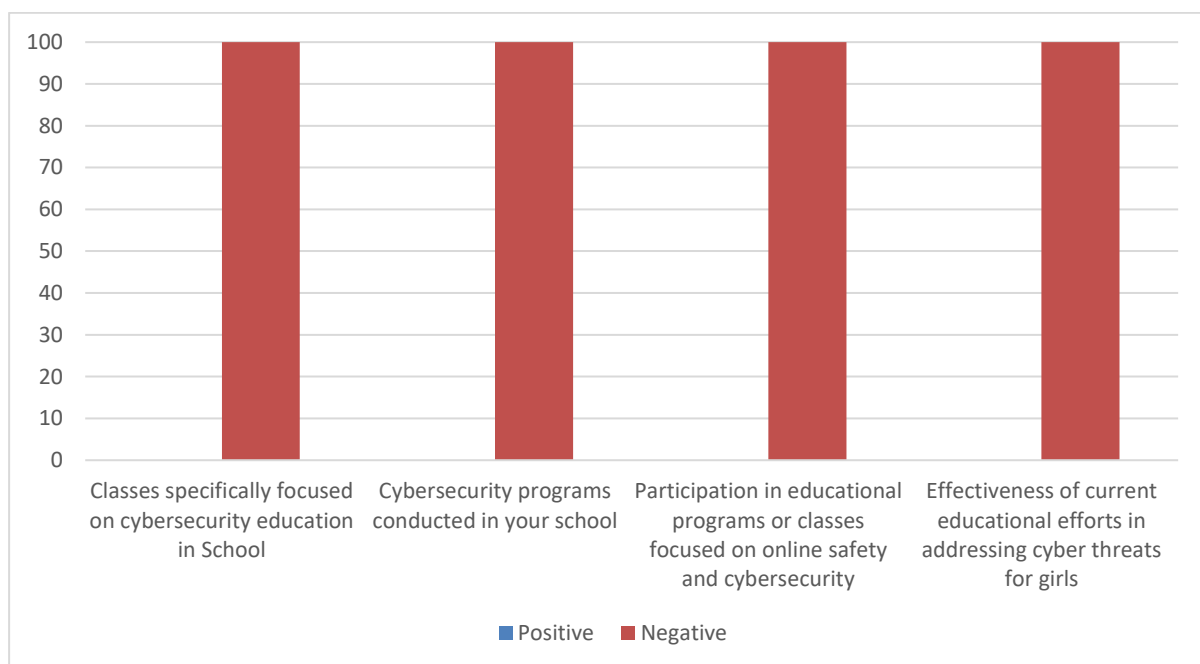


Figure 1.11

Cent percent of the respondents have said that school does not conduct any special classes or programs focused on cybersecurity education and none of the respondents have participated in educational programs or classes focused on online safety and cybersecurity outside school.

All the respondents have said that the current educational efforts in addressing cyber threats for girls are not effective at all.

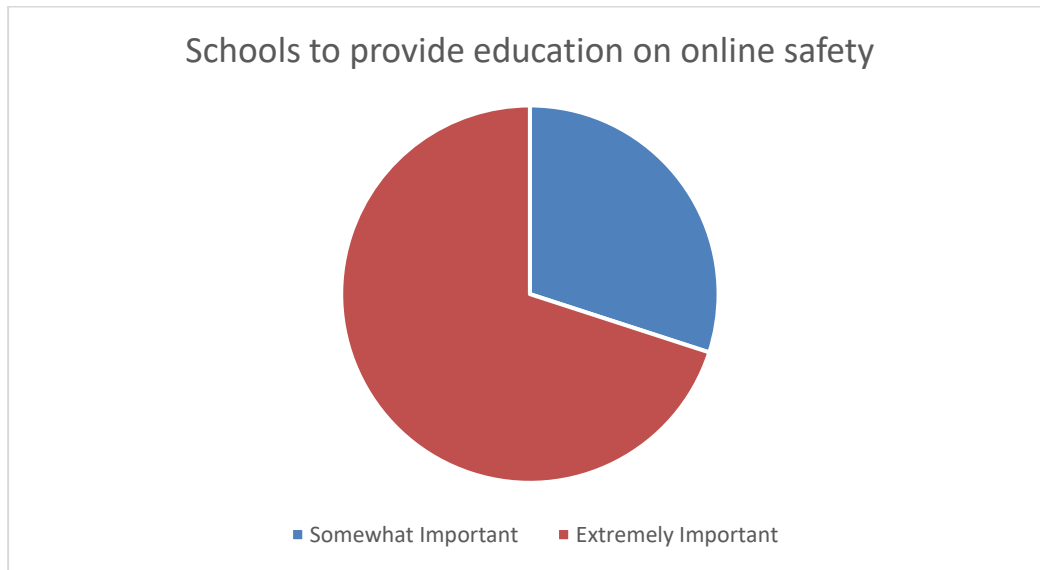


Figure 1.12

A vast majority of the respondents (70%) think that it is extremely important for schools to provide education on online safety and cybersecurity and 30% think that it is somewhat important for schools to provide education on online safety. And cent percent of the respondents said that the teachers should play a more active role in educating adolescents about cybersecurity.

VI. Parental Involvement

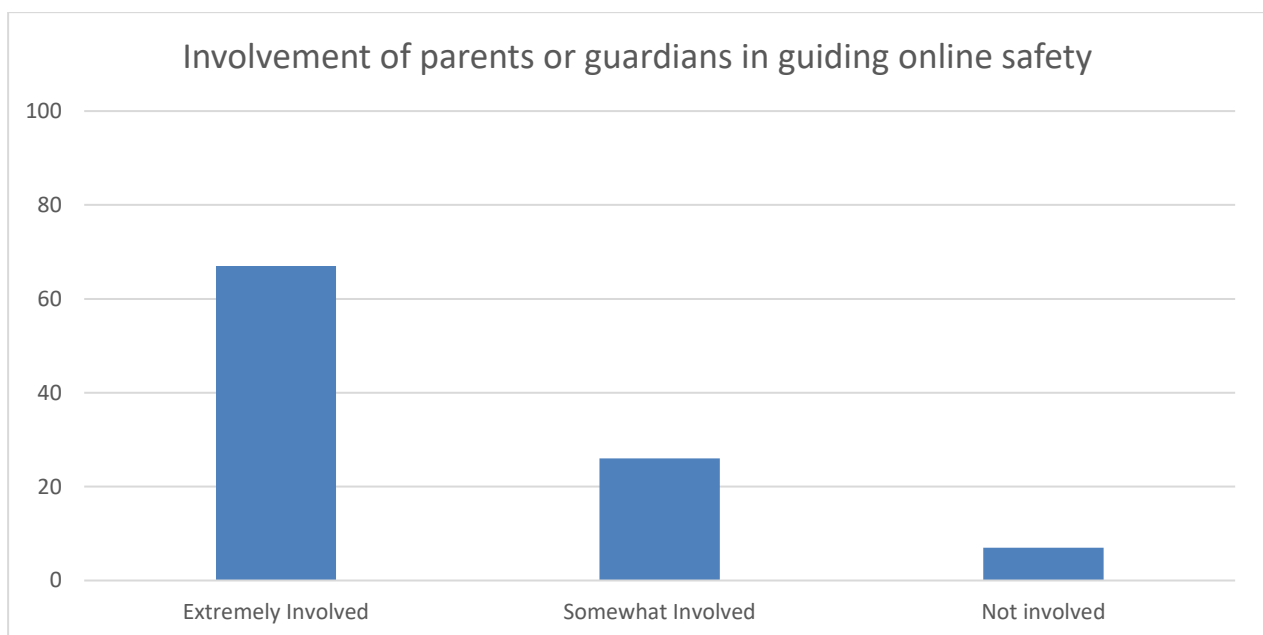
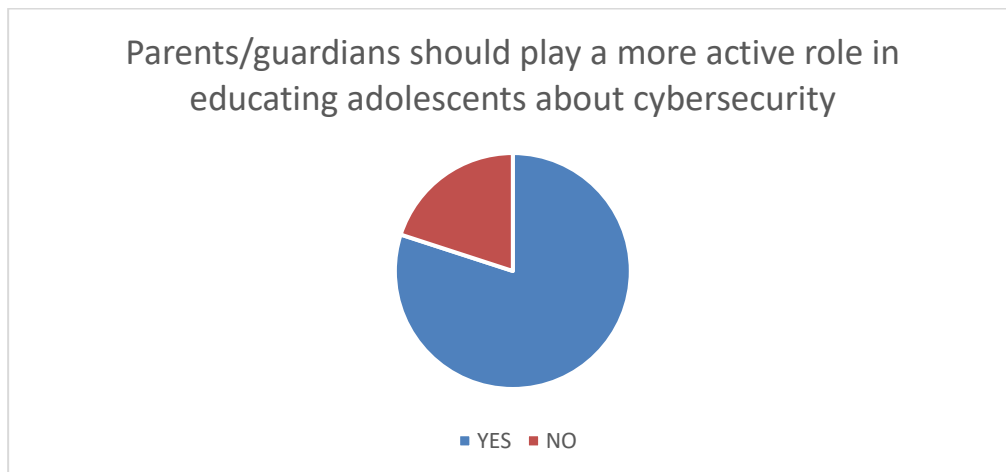
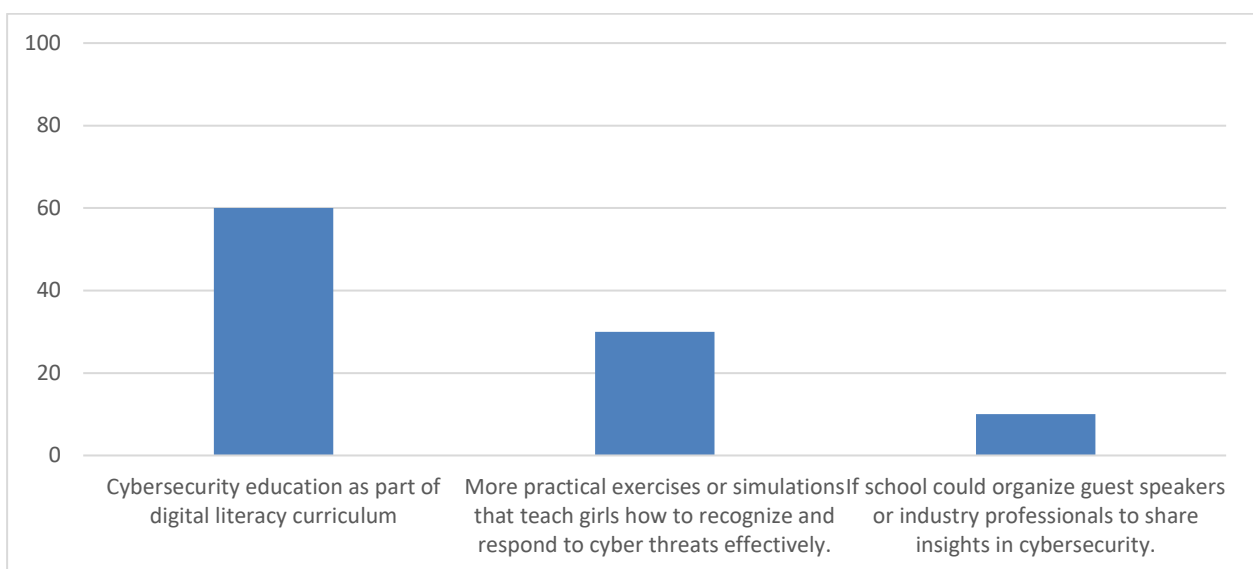


Figure 1.13

Majority of the respondents (67%) have said that their parents or guardians are extremely involved in guiding them regarding online safety. 26% have said that their parents or guardians are somewhat involved and 7% have said that they are not involved at all.

**Figure 1.14**

A vast majority of the respondents have (80%) said that parents/guardians should play a more active role in educating adolescents about cybersecurity and 20% parents/guardians should not play a more active role rather they should play a passive role in educating adolescents about cybersecurity.

**Figure 1.15**

More than half of the respondents (60%) have said that they would like if cybersecurity education becomes a part of digital literacy curriculum. 30% have said that if there are more practical exercises or simulations that teach girls how to recognize and respond to cyber threats effectively. 10% have said that it would be helpful if school could organize guest speakers or industry professionals to share insights in cybersecurity.



DATA INTERPRETATION - TEACHERS

I. Demographic Information

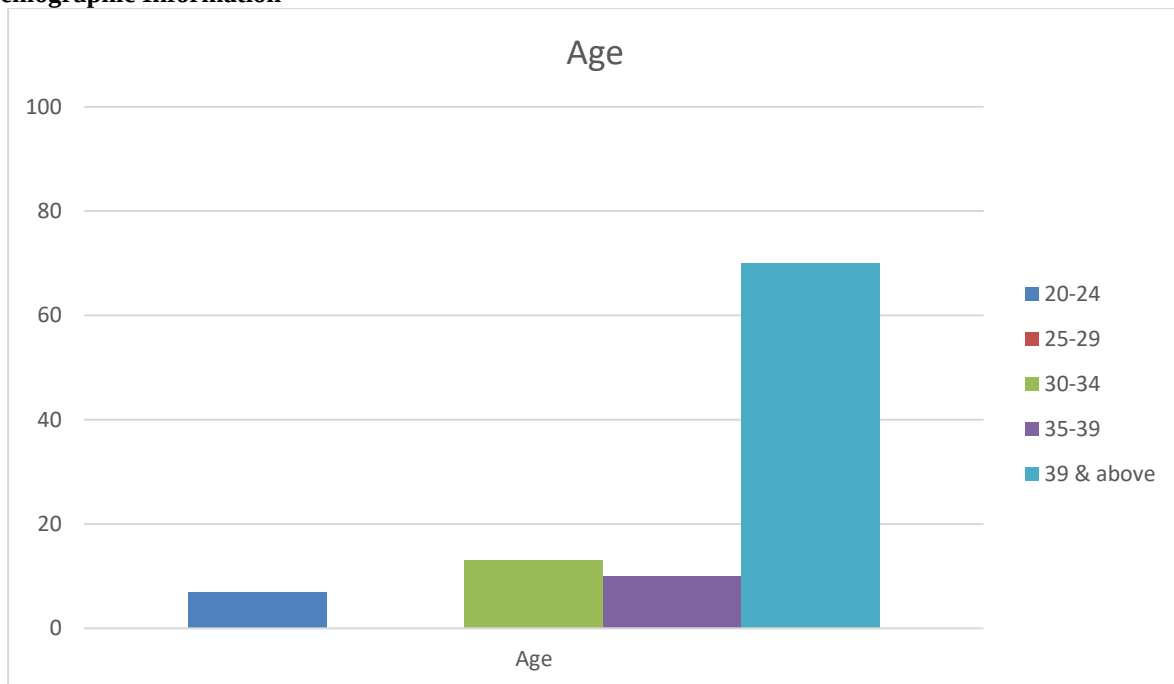


Figure 2.1

Majority (70%) of teachers belong to 39 & above age group, 13% belongs to 30-34 age group, 10% belongs to 35-39 age group, 7% belongs to 20-24 age group, none of them belongs to 25-29 age group.

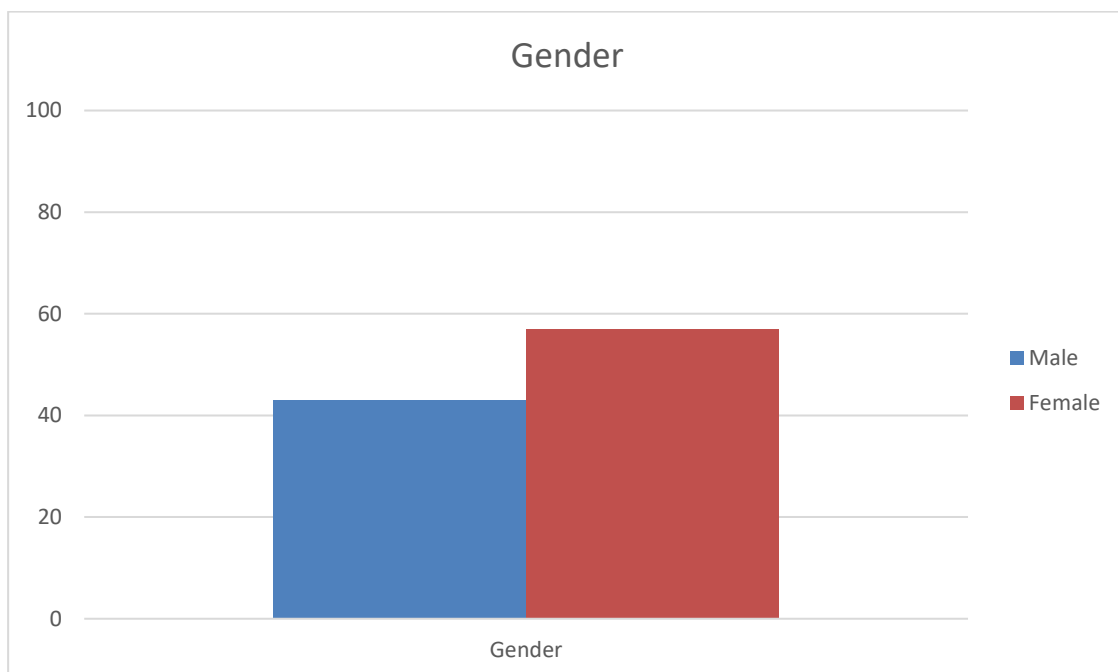
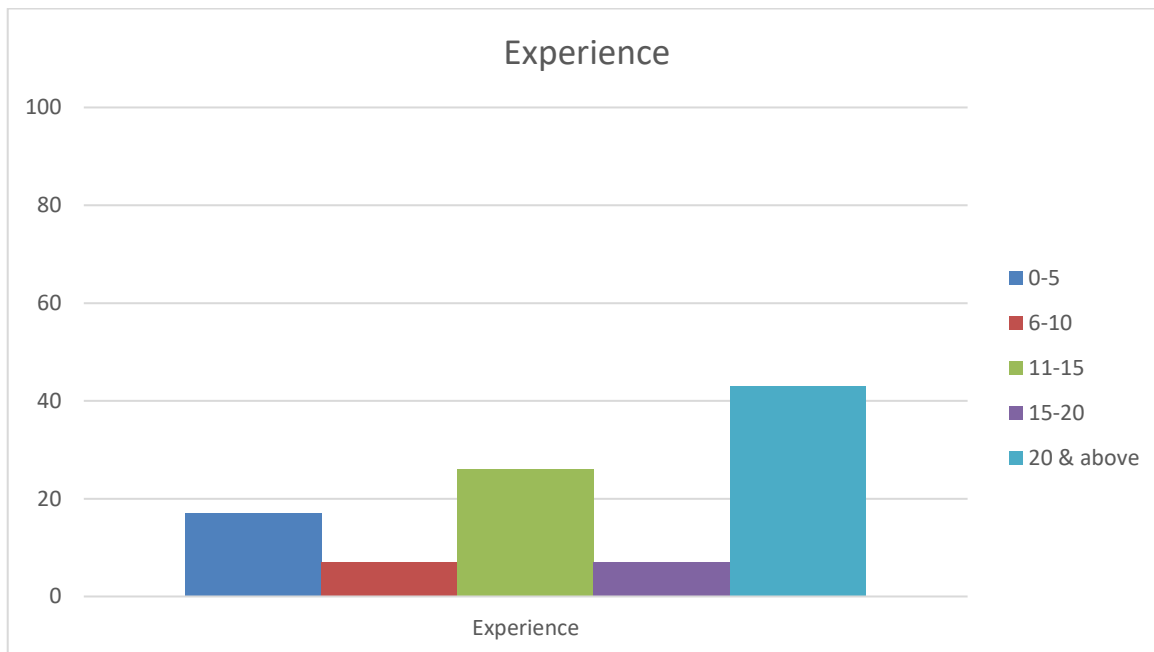


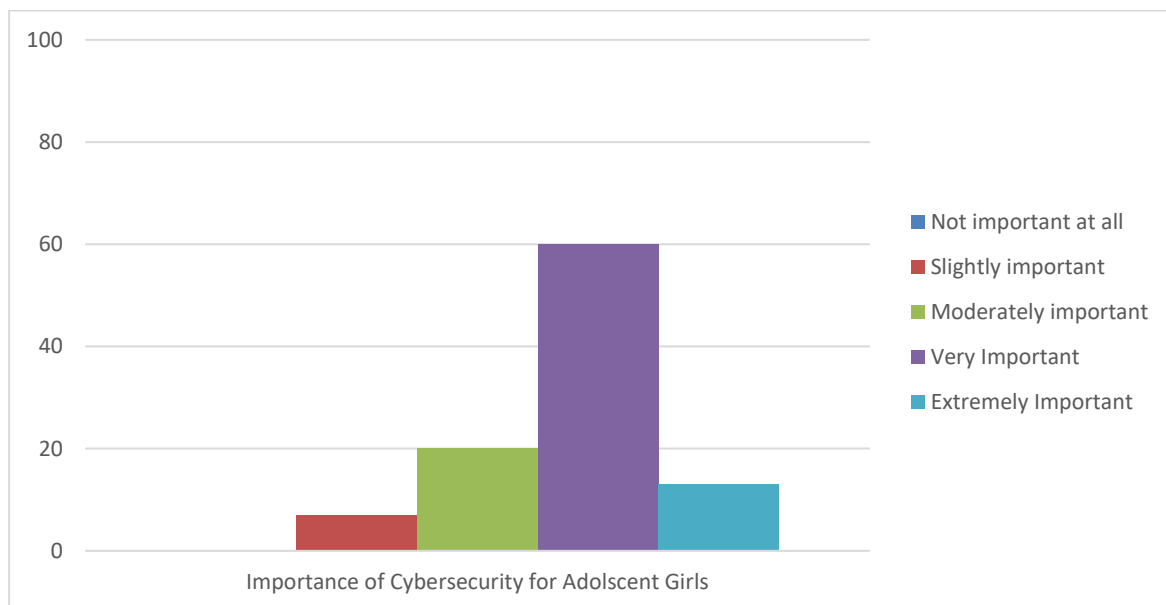
Figure 2.2

More than half of the respondents (57%) are Female. 43% are male.

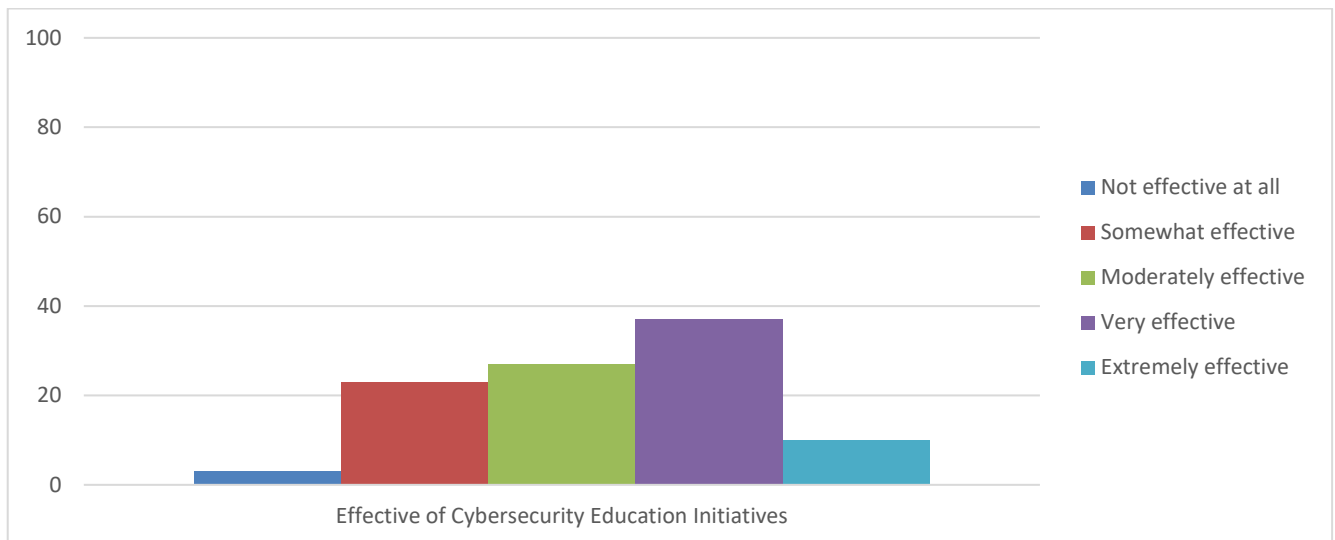
**Figure 2.3**

A vast proposition (43%) of teachers having 20 and above years of experience, 26% having 11-15 years of experience, 17% having 0-5 years of experience, 7% having 6-10 years and another 7% having 15-20 years of experience.

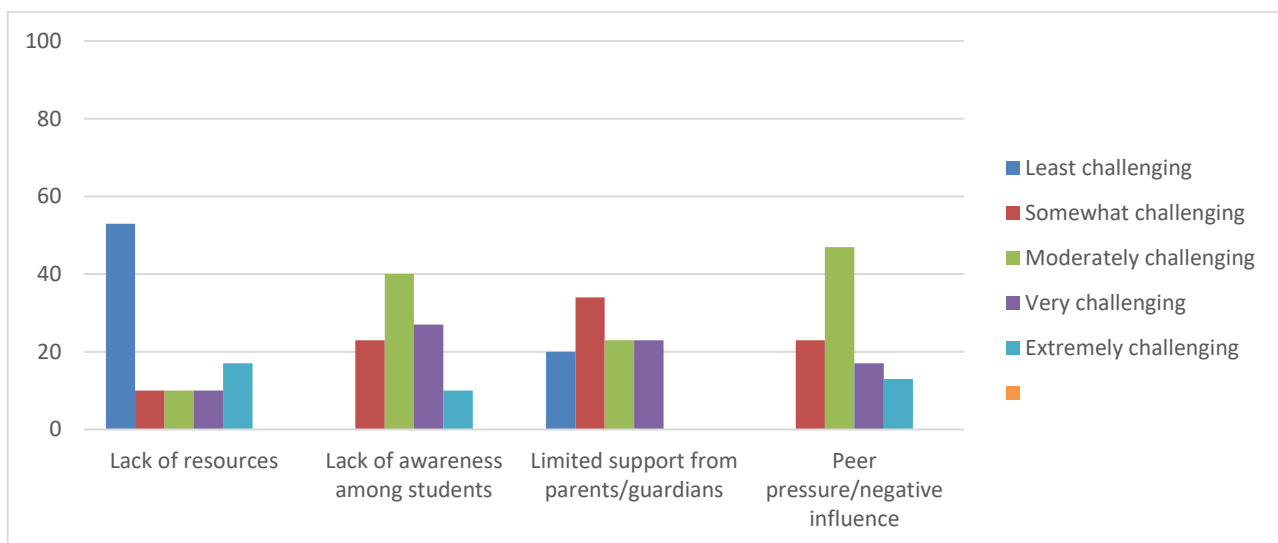
II. Perceptions of Cybersecurity Education

**Figure 2.4**

When asked about how important do you consider cybersecurity education for adolescent girls 60% of teachers said they consider cybersecurity is very importance for adolescent girls, 20% said moderately important, 13% said extremely important and 7% said slightly important.

**Figure 2.5**

When asked about how effective do you believe current cybersecurity education initiatives are for girls, 37% of teachers said very effective, 27% said moderately effective, 23% said slightly effective, 10% said extremely effective and 3% said not effective at all.

**Figure 2.6**

When asked about please rate the common challenges faced in teaching adolescent girls about online safety and cybersecurity.

- Lack of resources: 53% of teachers said least challenging, 10% said somewhat challenging, 10% said moderately challenging, 10% said very challenging and 17% said extremely challenging.
- Lack of awareness among students: 40% of teachers said moderately challenging, 27% said very challenging, 23% said somewhat challenging and 10% said extremely challenging.
- Limited support from parents/guardians: 34% of teachers said somewhat challenging, 23% said moderately challenging, 23% said very challenging and 20% said least challenging.
- Peer pressure/negative influence: 47% of teachers said moderately challenging, 23% said somewhat challenging, 17% said very challenging and 13% said extremely challenging.

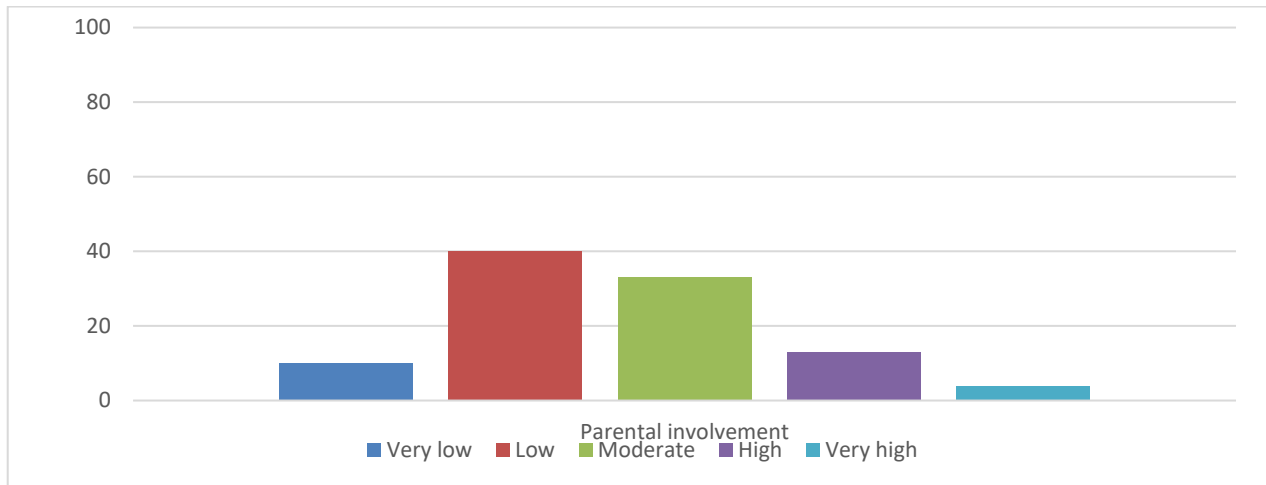


Figure 2.7

When asked about how would you rate the level of parental involvement in reinforcing cybersecurity education for girls, 40% of teachers said low level of parental involvement, 33% said moderately, 13% said high, 10% said very low and 4% said very high.

III. Experience with Educational Initiatives

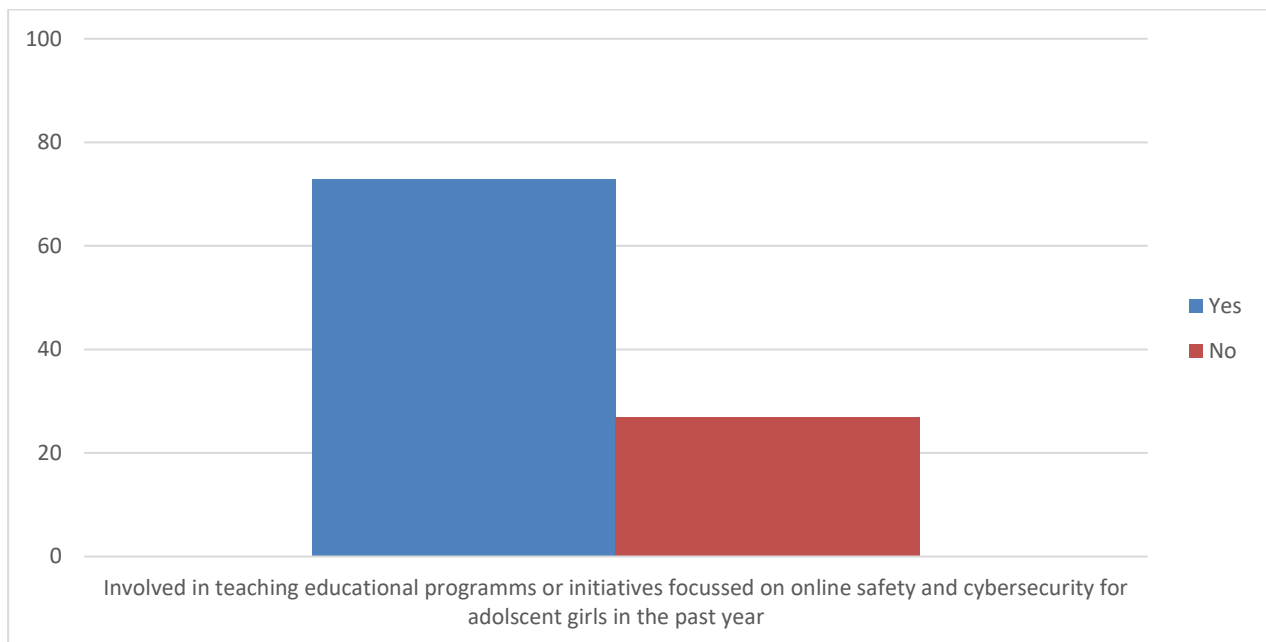


Figure 2.8

When asked about have you been involved in teaching educational programmes or initiatives focussed on online safety and cybersecurity for adolescent girls in the past year, 73% of teachers said Yes and 27% said No.

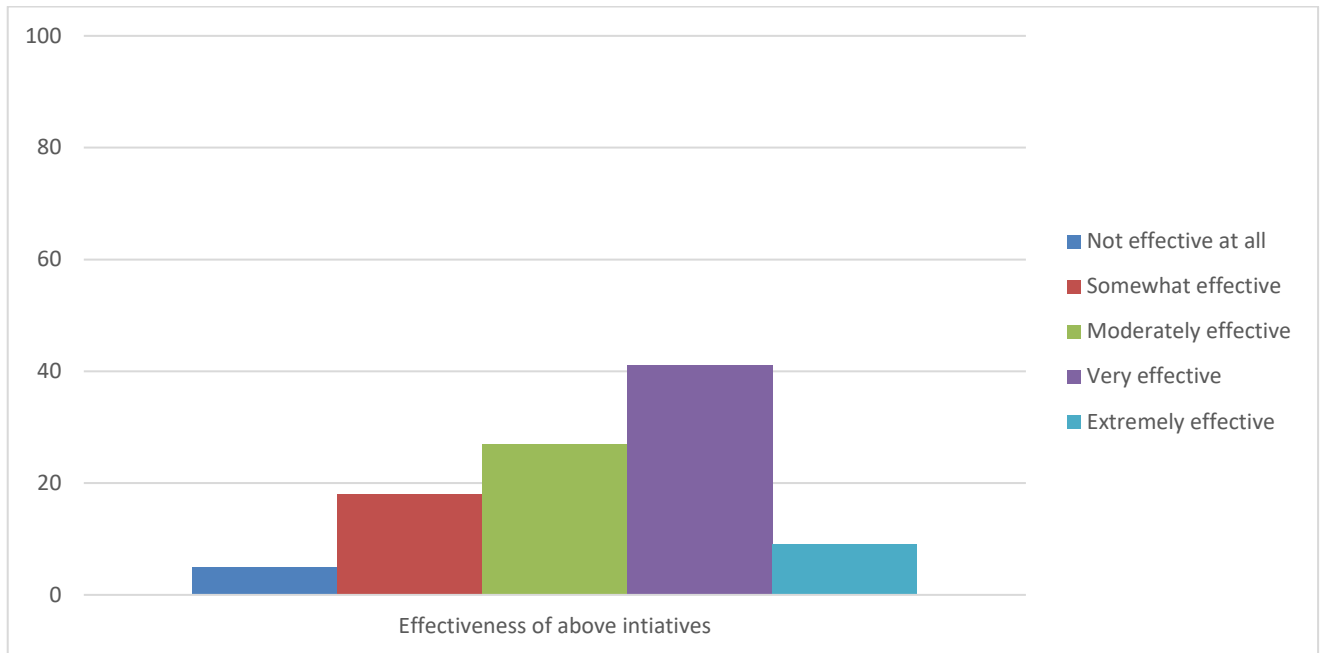


Figure 2.9

When asked about how effective do you find the above initiatives, 41% of teachers said very effective, 27% said moderately effective, 18% said slightly effective, 9% said extremely effective and 5% said not effective at all.

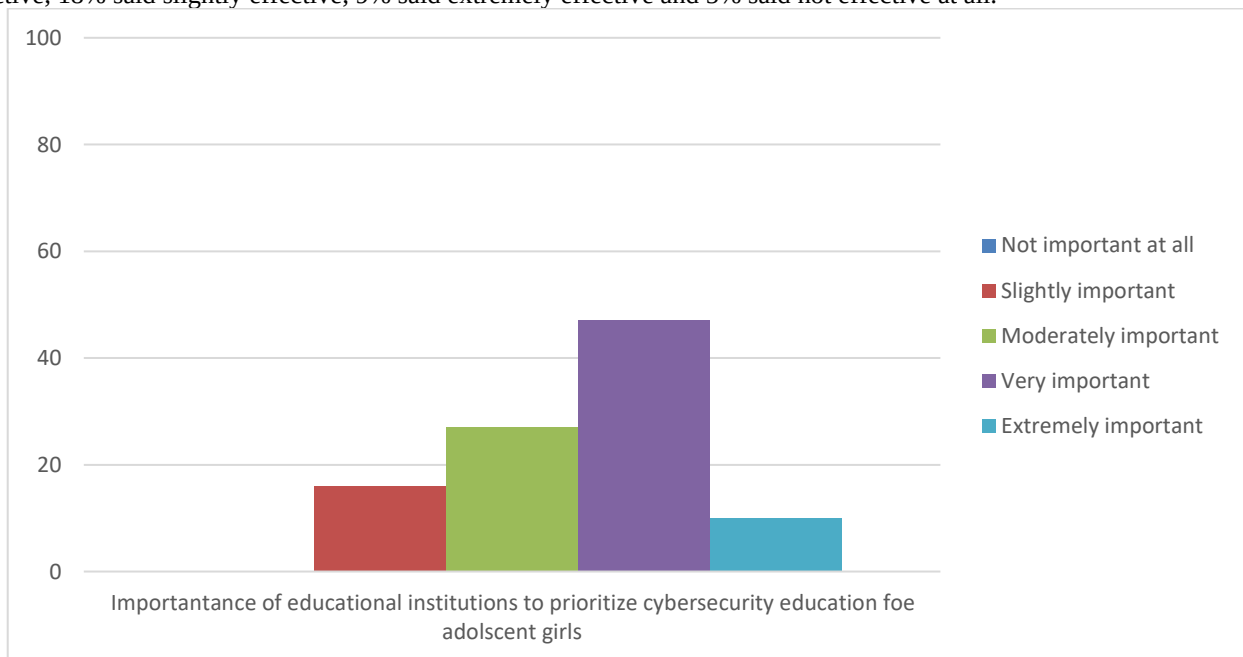
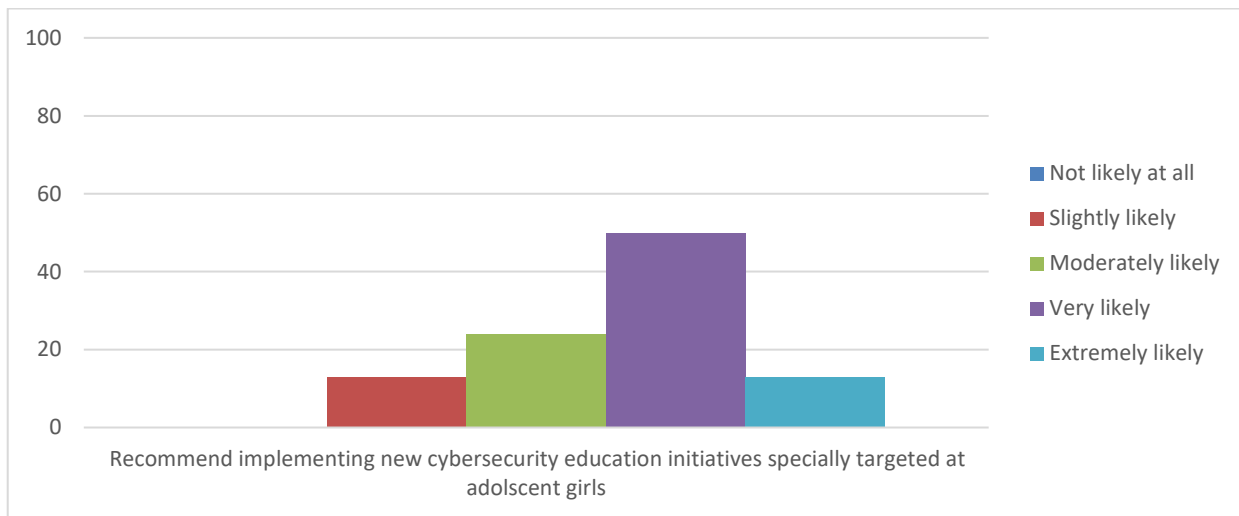
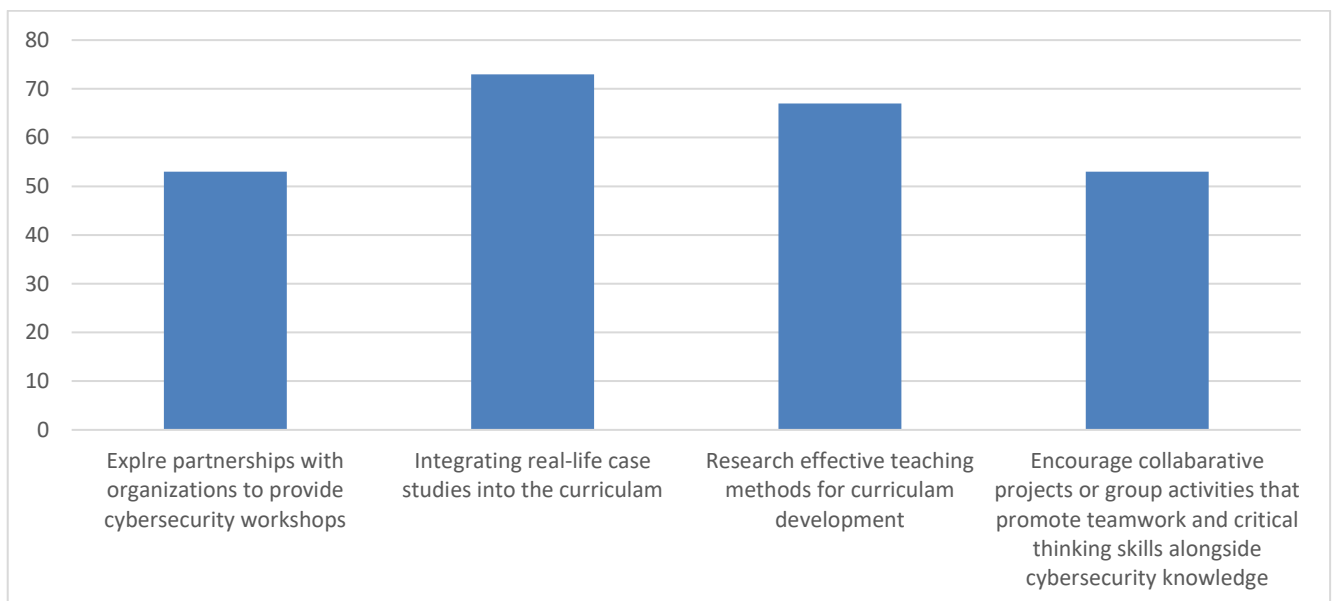


Figure 2.10

When asked about how important do you think it is for educational institutions to prioritize cybersecurity education for adolescent girls, 47% of teachers said very important, 27% said moderately important, 16% said slightly important. 10% said extremely important.

**Figure 2.11**

When asked about how likely are you recommend implementing new cybersecurity education initiatives specially targeted at adolescent girls in your school, 50% of teachers said very likely, 24% said moderate likely, 13% said slightly likely and another 13% said extremely likely.

**Figure 2.12**

When asked about is there anything else you would like to add regarding cybersecurity education for adolescent girls, 53% of teachers said explore partnerships with organizations to provide cybersecurity workshops, 73% said integrating real-life case studies into the curriculum, 67% said research effective teaching methods for curriculum development, 53% said encourage collaborative projects or group activities that promote teamwork and critical thinking skills alongside cybersecurity knowledge.

MAJOR FINDINGS

The findings suggest that students are using internet for long hours in a day mainly for studies and social interactions. This extensive usage of internet makes it necessary that the students are equipped with necessary skills to handle the digital world with safety. It was observed that respondents mainly in the age group of 15-16 were not using social media, the main reasons being restriction from parents and studies. It was also observed that respondents who are using social media mainly who post content are confident in their ability to navigate online threats and stay safe on the internet. But at the same time, they also express some level of worry.

The experience with cyberbullying and online harassment, reported by 30% of respondents, indicates that these issues are significant among the student population. Majority of the respondents have low confidence levels on how to navigate these issues and that is why there is immense need for cybersecurity education. Even though teachers are involved in teaching about online



safety and cybersecurity for adolescent girls in the past year, it is alarming to note that there is absence of formal cyber education, especially given the high levels of internet engagement among students.

Mostly students are learning about online safety from experiences around them or through news articles. That is why the call for increased active roles by both parents and teachers indicates that students seek a more collaborative and supportive approach to learning about cybersecurity. The findings also highlight that parents are involved in students' life of their usage in devices by entirely restricting them from using but they are as involved in guiding the children about online safety.

The majority, both among students and teachers are favouring that school should take a active role in implementing new cybersecurity education initiatives specially targeted at adolescent girls in school as the effectiveness of the cyber education is not on par with the evolving usage of internet among students. Real life experiences and workshops with industrial experts and guest speakers on cyber security education is being preferred along with formal cyber security education in digital curriculum.

SUGGESTIONS

- Schools should incorporate a formal and detailed cyber security syllabus into their curriculum.
- The curriculum should include basic knowledge on how to recognize and respond to cyber threats, and also understanding privacy settings on social media.
- Teachers should be provided additional training to ensure that they are also well equipped with sufficient knowledge to educate students on cybersecurity
- Parent- teacher workshops can be conducted to encourage parents to play an active role in their children's online safety education.
- A student guidance counsellor can be appointed for students who have or are facing any cyber threats.
- Invite cyber security experts to share insights and real-life experience with students.
- Explore partnerships with cybersecurity organizations to provide workshops, resources, and support for implementing effective cybersecurity education programs.

CONCLUSION

With the dynamic and evolving nature of the digital technology in education, The National Education Policy 2020 emphasized the integration of cyber safety education. In the school curriculums. But even after four years there is a significant gap in formal cybersecurity education in many schools. By highlighting the critical role of education in empowering girls to navigate cyber threats this study highlights the importance of integrating comprehensive cybersecurity modules into the school curriculum. Additionally, both teachers and students are expecting need for increased parental involvement and practical exercises to enhance students' understanding of cyber threats and on how to navigate them properly. By addressing these gaps educational institutions can create a safer and more informed digital environment for adolescent girls.

REFERENCES

1. Akinola, O. (2023). *How to help SMEs scale production with adequate cyber education*. *Journal of Knowledge Learning and Science Technology* Issn 2959-6386 (Online), 1(1), 185-190. <https://doi.org/10.60087/jklst.vol2.n2.p190>
2. Berlilana, Tim Noparumpa, Athapol Ruangkanjanases, Taqwa Hariguna, and Sarmini. (2021). *Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness*. *Sustainability* 13, no. 24: 13761. <https://doi.org/10.3390/su132413761>
3. Balabantaray, Subhra & Mishra, Mausumi & Pani, Upananda. (2023). *A Sociological Study of Cybercrimes Against Women in India: Deciphering The Causes And Evaluating The Impact On The Victims*. *International Journal of Asia Pacific Studies*. 19. 23-49. 10.21315/ijaps2023.19.1.2.
4. Casey, E., Jocz, J., Peterson, K., Pfeif, D., & Soden, C. (2023). *Motivating youth to learn stem through a gender inclusive digital forensic science program*. *Smart Learning Environments*, 10(1). <https://doi.org/10.1186/s40561-022-00213-x>
5. *Crime in India*. (2022). National Crime Records Bureau. <https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf>
6. *Increase In Cyber Crimes*.(2024). Press Information Bureau. <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505>
7. FAMILONI, B. (2024). *Cybersecurity challenges in the age of ai: theoretical approaches and practical solutions*. *Computer Science & It Research Journal*, 5(3), 703-724. <https://doi.org/10.51594/csitrj.v5i3.930>
8. Hattar-Pollara, M. (2019). *Barriers to education of Syrian refugee girls in Jordan: gender-based threats and challenges*. *Journal of Nursing Scholarship*, 51(3), 241-251. <https://doi.org/10.1111/jnu.12480>
9. Jethwani, M., Memon, N., Seo, W., & Richer, A. (2016). "I can actually be a super sleuth". *Journal of Educational Computing Research*, 55(1), 3-25. <https://doi.org/10.1177/0735633116651971>
10. Kanchana, Dr & Y, Ms & M, Ms & J, Ms. (2022). *Cyber Crimes and Cyber Hygiene Practices Among Young Girls*. *International Journal of Advanced Research in Science, Communication and Technology*. 568-574. 10.48175/IJARSC-7322.
11. Kangwana, B., Muthengi, E., & Austrian, K. (2020). *Intra-grade variability in educational and psychosocial competencies of school going adolescent girls, in the coastal region of kenya: implications for school based interventions*. *BMC Public Health*, 20(1). <https://doi.org/10.1186/s12889-020-09097-3>
12. Kashyap, S. (2024). *The influence of artificial intelligence on cybersecurity*. *International Journal of Innovative Research in Computer and Communication Engineering*, 12(Special Is), 13-22. <https://doi.org/10.15680/ijirce.2024.1203503>



13. Koffman, O. and Gill, R. (2013). 'the revolution will be led by a 12-year-old girl': girl power and global biopolitics. *Feminist Review*, 105(1), 83-102. <https://doi.org/10.1057/fr.2013.16>
14. Kyva, V., Zastelo, O., & Nakonechnyi, O. (2022). Formation of cyber security skills through methods of hacking, bypassing and protecting the procedure for granting access in microsoft windows operating system. *Information Technologies and Learning Tools*, 89(3), 233-248. <https://doi.org/10.33407/itlt.v89i3.4949>
15. Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Safe and responsible internet use in a connected world: promoting cyber-wellness. *Canadian Journal of Learning and Technology*, 47(4). <https://doi.org/10.21432/cjlt28069>
16. Marphatia, A., Ambale, G., & Reid, A. (2017). Women's marriage age matters for public health: a review of the broader health and social implications in south Asia. *Frontiers in Public Health*, 5. <https://doi.org/10.3389/fpubh.2017.00269>
17. Noparumpa, T., Ruangkanjanases, A., & Hariguna, T. (2021). Organization benefit as an outcome of organizational security adoption: the role of cyber security readiness and technology readiness. *Sustainability*, 13(24), 13761. <https://doi.org/10.3390/su132413761>
18. NS Sulaiman. (2023). Cyber security awareness model (among children) using protection motivation theory: a review. *International Journal of Business and Technology Management*. <https://doi.org/10.55057/ijbtm.2023.5.s5.9>
19. Shroff, M., Griffiths, P., Adair, L., Suchindran, C., & Bentley, M. (2008). Maternal autonomy is inversely related to child stunting in andhra pradesh, india. *Maternal and Child Nutrition*, 5(1), 64-74. <https://doi.org/10.1111/j.1740-8709.2008.00161.x>
20. Sonhera, N., Kritzinger, E., & Looock, M. (2021). Cyber incident handling and the perceptions of learners on cyber incidents in south african schools. *Advances in Science Technology and Engineering Systems Journal*, 6(5), 23-31. <https://doi.org/10.25046/aj060504>
21. Visakhapatnam district reported 621 cybercrime cases in 2022, highest in Andhra Pradesh: NCRB data. (2023). *The Hindu*. <https://www.thehindu.com/news/cities/Visakhapatnam/visakhapatnam-district-reported-621-cybercrime-cases-in-2022-highest-in-andhra-pradesh-ncrb-data/article67618594.ece>