AMERICAN JOURNAL OF EDUCATION AND TECHNOLOGY (AJET)

ISSN: 2832-9481 (ONLINE)

VOLUME 2 ISSUE 4 (2023)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Education and Technology (AJET)

Volume 2 Issue 4, Year 2023
ISSN: 2832-9481 (Online)
DOI: https://doi.org/10.54536/ajet.v2i4.2248
https://journals.e-palli.com/home/index.php/ajet

Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province

Abdul Wajid Fazil[1], Musawer Hakimi[2*], Saidamin Sajid[3], Mohammad Mustafa Quchi[4], Khudai Qul Khaliqyar[3]

Article Information

Received: October 16, 2023
Accepted: November 19, 2023
Published: November 24, 2023

Keywords

Cybersecurity Education, Digital Literacy, Online Safety, Internet Privacy, Information Security, Youth Empowerment, Educational Strategy

ABSTRACT

In the contemporary digital era, the pervasive influence of the internet underscores the imperative to equip the youth with skills for secure online navigation. While the internet presents vast opportunities, it simultaneously exposes young learners to potential risks, encompassing cyberbullying, privacy breaches, and security threats. This research meticulously examines the impact of cybersecurity education on the digital literacy and online safety of students, emphasizing the youth in Badakhshan Province, Afghanistan. It advocates for the cultivation of digital literacy and online safety principles across diverse age groups and fields of study. Furthermore, the study underscores the paramount importance of instilling awareness regarding responsible digital practices related to privacy, security, and copyright, with a compelling call for active parental involvement. To execute this research, a robust stratified random sampling technique was deployed, meticulously selecting 170 male and female students from various grade levels in both public and private schools within Badakhshan province, Afghanistan. Data collection was facilitated through a comprehensive survey questionnaire featuring 16 Likert scale-based questions. Subsequently, the gathered data underwent rigorous statistical analysis, encompassing descriptive and inferential statistics, regression analysis, and qualitative content analysis. This research yields invaluable insights into the internet behavior and cybersecurity awareness of the youth in Badakhshan Province, Afghanistan. It makes essential contributions to comprehending their online activities and digital literacy. The overarching goal is to empower students to navigate the digital landscape with confidence and ethical discernment by integrating cybersecurity education into school curricula. This approach not only safeguards their privacy and security but also optimizes the internet's full potential. The study significantly contributes to fostering a safer, more responsible, and knowledge-driven society.

INTRODUCTION

In an era marked by increasing digitization, the imperative of enhancing internet safety and cybersecurity awareness among secondary and high school students cannot be overstated. As technology becomes deeply integrated into various aspects of daily life, equipping the youth with the knowledge and skills to navigate the digital landscape securely is paramount. Reflecting the global trend of addressing cybersecurity education in educational curricula, particularly in regions such as Badakhshan Province, Afghanistan, underscores the necessity of proactive measures (Valcheva, 2020). Although the prevalence of cyber threats in this region may not be as alarming as in some other parts of the world, the ever-evolving nature of cyber threats necessitates ensuring that students are well-prepared to safeguard themselves and their information online. The state of cybersecurity awareness and education in Afghanistan, particularly in secondary and high schools, emerges as a subject of critical concern. While various countries, exemplified by the Government of the United Kingdom (2020) and the Japan Ministry of Education (2017), have taken significant steps in integrating cybersecurity education into their educational systems, Afghanistan faces unique challenges and opportunities. The lack of cybersecurity awareness and education can expose students to risks such as cyberbullying, online scams, and other harmful online activities, underscoring the need for immediate action (Jones & Brown, 2020). As the government and educational institutions in Afghanistan work towards addressing these challenges, it becomes crucial to examine existing practices, strategies, and potential areas of improvement in enhancing internet safety and cybersecurity awareness among secondary and high school students in Badakhshan Province. This case study aims to shed light on the current state of cybersecurity education in the region, analyze the effectiveness of different approaches, and offer insights that can inform the development of standardized guidelines for incorporating cybersecurity education into school curricula, aligning with global imperatives (Valcheva, 2020). Furthermore, this study underscores the importance of a holistic approach to cybersecurity education, emphasizing technical skills, ethical values, and responsible digital citizenship (Livingstone & Bulger, 2014). Nurturing a new generation of informed digital citizens capable of navigating the digital world responsibly and safely is essential. Through collaboration among schools, parents, and the local community, the goal is to create a safer digital environment for secondary and

[1] Department of IS, Badakhshan University, Afghanistan
[2] Department of Computer Science, Samangan University, Afghanistan
[3] Department of IT, Badakhshan University, Afghanistan
[4] Department of Network Engineering, Faryab University, Afghanistan
[*] Corresponding author's e-mail: musawer@adc.edu.in

high school students in Badakhshan Province, equipping them with the necessary tools and knowledge to engage with technology securely and ethically. This case study sets the stage for an in-depth examination of the current landscape of cybersecurity education in Badakhshan Province, Afghanistan, and the strategies employed to enhance internet safety and cybersecurity awareness among secondary and high school students. Through this research, we seek to contribute to the global imperative of fostering a safer digital environment and empowering the youth with the knowledge and skills they need to thrive in an increasingly connected world.

Significance of The Study

The significance of this research lies in the critical need for enhanced cybersecurity awareness and education in our increasingly digital world. Cybersecurity is a pressing concern, and the escalating frequency and complexity of cyber threats underscores its significance. The existing knowledge gap among the general population and students, in particular, emphasizes the importance of this research. By incorporating cybersecurity education into school curricula, we address the dire need for cyber literacy from an early age. Furthermore, this study contributes significantly to academic knowledge by bridging the gap between the education sector and the cybersecurity domain. It offers an innovative approach by advocating for cybersecurity integration within formal education systems, making it an essential part of academic discourse. This research proposes practical solutions, aligning academic endeavors with real-world challenges. Moreover, the study serves as a reference for policymakers, educators, and institutions interested in cybersecurity education, as it provides a comprehensive blueprint for implementation. It offers insights into optimizing knowledge transfer to create a safer digital environment, reducing vulnerabilities and enhancing cyber resilience. Ultimately, the research explores uncharted territories at the intersection of cybersecurity and education, opening doors for further academic inquiry and innovative strategies to bolster cybersecurity. This study's findings are instrumental in addressing the growing threat of cyberattacks and fortifying the global digital landscape.

LITERATURE REVIEW

Cybersecurity education for young learners has gained prominence in the wake of an increasingly digitized world. This vital aspect of modern education ensures that young individuals can safely and responsibly navigate the digital landscape. The ever-evolving nature of cyber threats underpins the importance of this education. Smith *et al.* (2018) emphasize the significance of imparting digital literacy and cybersecurity skills to the younger generation. Their research aligns with the global trend of integrating cybersecurity into educational curricula, highlighting that schools need to create a safer digital environment for students. Jones and Brown (2020) reiterate the need for cybersecurity education, noting the potential risks young individuals face, including cyberbullying, online scams, and other harmful activities. Education in this context becomes a proactive measure against such threats. It imparts technical skills and fosters a sense of empowerment among students (Li *et al.*, 2019). International practices set an example for cybersecurity education integration. Countries like the United Kingdom, Japan, and India have already taken significant steps in this direction. The government of the United Kingdom (2020) has emphasized the need for a proactive approach to cybersecurity education, aligning with the objectives of the National Cyber Security Policy (2013). Japan, through its Ministry of Education (2017), has similarly incorporated cybersecurity into its educational systems, emphasizing the global need for such programs. A holistic approach to cybersecurity education emphasizes technological skills, ethical values, and digital citizenship (Livingstone & Bulger, 2014). Cybersecurity education should be viewed as an indispensable component of modern education, equipping young learners with the tools and knowledge to engage with technology safely and responsibly. Cybersecurity education, as emphasized by Smith *et al.* (2018) and Jones and Brown (2020), is essential to address the evolving threats in the digital age. Students, now more than ever, need to be equipped with the knowledge and skills to protect themselves and their information online. Cybersecurity education doesn't just prevent individuals from falling victim to cyber threats; it also cultivates a sense of responsibility and ethical behavior. The study conducted by Li *et al.* (2019) aligns with these principles by advocating for the integration of cybersecurity into educational frameworks. It recognizes that the threats faced by students are not limited to mere technological challenges but encompass the complexities of the digital world, such as privacy concerns and ethical dilemmas.

One key aspect of these discussions is the collaborative effort required between schools and parents. Anderson and Milfont (2017) highlight the crucial role parents play in guiding their children to practice safe and responsible online behavior. Parents' involvement in their children's cybersecurity education strengthens the impact of educational initiatives. As the research demonstrates, the implementation of comprehensive cybersecurity education has been successful in various countries. The United Kingdom, Japan, and India's proactive approach (Government of the United Kingdom, 2020; Japan Ministry of Education, 2017; National *et al.* Policy, 2013) can serve as models for other nations. It emphasizes the global need for comprehensive cybersecurity education to foster a safer digital environment. Livingstone and Bulger (2014) underscore the multifaceted nature of cybersecurity education, focusing on not only the practical skills but also the ethical values and digital citizenship it promotes. This approach aligns with the broader goal of nurturing responsible and aware digital citizens who can safely navigate the digital landscape. In summary, the

existing cybersecurity education literature consistently highlights this educational component's urgency and significance in the digital age. By integrating cybersecurity into curricula and involving both schools and parents, we can effectively prepare young learners to tackle the challenges and opportunities of the digital world. These insights should guide educational policies to promote safe, responsible, and ethical digital practices among the younger generation.

Objectives of The Study

• To assess the current level of internet usage and online activities of secondary and high school students in Badakhshan Province, Afghanistan, with a focus on gender and age groups.

• To investigate the average time students, spend on the internet daily and identify variations based on gender and age categories.

• To determine the most common online activities engaged in by students, emphasizing platforms such as Facebook, online gaming, educational content, YouTube, and streaming services.

• To analyze students' preferred internet access devices, including desktop computers, laptops, smartphones, and tablets, and examine any potential associations with their online behavior.

• To identify the physical locations where students access the internet, differentiating between home, internet cafes, public places, and schools.

• To understand students' perceptions of the importance of internet usage for their studies and daily lives and explore whether they believe excessive internet usage is a concern.

• To investigate students' awareness of cybersecurity issues, their experiences of cyber threats or incidents, and their responses to such incidents.

MATERIALS AND METHODS

Population and Sample: In this research, the study population encompasses students spanning multiple grade levels, encompassing 6th, 7th, 8th, 9th, 10th, and 11th and 12th grades, attending public and private schools within Badakhshan province. The overall population size is characterized by the cumulative count of students enrolled across these diverse grade levels. For the purpose of this research "stratified random sampling technique" was employed to select a representative sample from this population. Stratification involved dividing the population into subgroups based on grade levels, ensuring a proportional representation of students from each grade. From each stratum, a random sample of students was selected. A sample size of 170 male and female students was determined based on a "confidence level of 95% and a margin of error of 5%".

Statistical Techniques Used in the Present Study:The research methodology primarily employs The study utilizes a combination of qualitative and quantitative data analysis techniques to comprehensively investigate the state of cybersecurity awareness among students. Quantitative data was collected through a structured survey questionnaire. Descriptive statistics, including percentages and frequencies, were used to analyse and summarize the data. Cross-tabulation was employed to explore relationships and patterns within the data.

Qualitative data was gathered through open-ended questions in the survey, which were subsequently analysed using thematic analysis. The thematic analysis involved the identification of recurring themes and patterns within the qualitative responses provided by the students. Data collection involves a Likert scale-based survey with 16 questions. Once the data has been pre-processed, statistical analyses will be performed using a range of methods. These analyses will include descriptive statistics to summarize the data and inferential statistics to examine variations based on gender and age groups. Additionally, qualitative content analysis will be conducted within the SPSS version 24 software. This comprehensive methodology aims to provide insights into students' internet behaviour, offering valuable contributions to understanding their online activities and cybersecurity awareness in Badakhshan Province, Afghanistan.

Data Analysis and Interpretation :The study conducted at Badakhshan province aimed Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study in Badakhshan Province, the study employed descriptive statistics and cross-tabulation for quantitative data, revealing variations in cybersecurity awareness among students of different grades and genders.

RESULTS AND DISCUSSION

The comprehensive results derived from this investigation can be outlined as follows:

Interpretation of Figure 1

The study covers a diverse range of ages among participants.

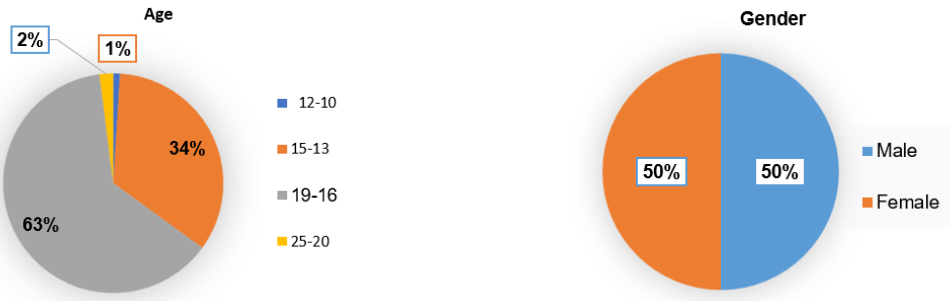

Figure 1: A diverse range of ages among participants

The majority, around 63%, are aged between 16 and 19. A smaller segment, approximately 1%, falls in the 13 to 15 age group. Overall, the study represents students aged 12 to 19. In terms of gender, it includes an almost equal distribution of males (50%) and females (50%).

Interpretation of Figure-2

Regarding electronic devices, nearly three-quarters of the students predominantly use smartphones, with a focus on 74% relying on them. Laptops constitute the second most popular choice among students, with 16% of the sample. Desktop computers are the least utilized devices, making up only 3% of the total participants.

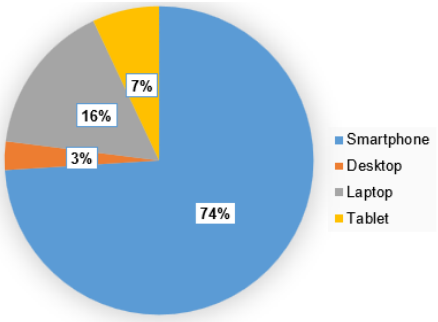

Figure 2: Electronic device usage

Interpretation of Figure-3

The figure below presents the findings of the study concerning the locations from which students primarily access the internet. It highlights that the majority of students, approximately 80%, predominantly access the internet from their homes. A smaller portion, about 8%, uses the internet in urban areas, while 5% do so in rural regions. Less than 1% (0.98%) relies on internet cafes for their internet access.

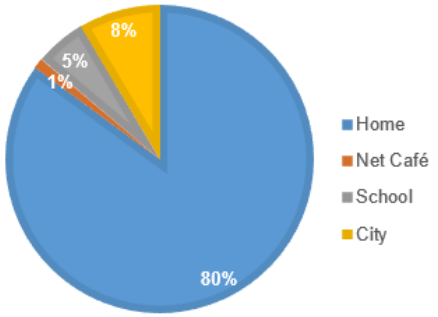

Figure 3: Internet access locations

Interpretation of Figure-4

The figure below provides insights into the internet usage patterns among students. It indicates that the majority of students, around 6%, spend 1-2 hours per day using the internet. Approximately 18% of the students do not use the internet at all. Meanwhile, 16% of the students are heavy internet users, spending 5-6 hours online daily.

Interpretation of Figure-5

The figure below illustrates the multifaceted role of the internet as a valuable tool for students. Among the surveyed participants, 39% utilize the internet for educational purposes, accessing study materials and resources. Social networking activities on Facebook are also prevalent, with 35% of students engaging in such interactions. Additionally, 15% turn to YouTube for various online content, while 11% participate in online gaming. This data emphasizes that internet usage among students extends beyond mere entertainment, highlighting its significance in facilitating education, social interaction, and entertainment.

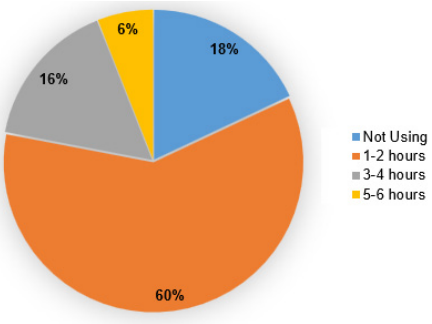

Figure 4: Internet usage duration

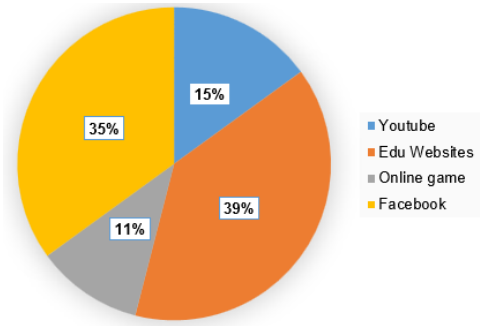

Figure 5: Internet usage activities

Interpretation of Figure-6, 7

The figure depicts that the internet serves as a versatile tool, providing a wide range of activities and benefits to students. Among the surveyed students, 36% use the internet for studying and accessing educational materials, 35% engage in social networking activities on Facebook, 15% utilize YouTube, and 11% participate in online gaming. This highlights that internet usage extends beyond mere entertainment, with a substantial number of students utilizing it for educational purposes, social interaction, and entertainment. The statistics prior to the awareness workshop were disheartening, but following the workshop, there was a notable improvement in students' awareness and their sense of online security. Specifically, 36.22% of students reported feeling very secure, 30.80% indicated increased security, and 14.80% expressed decreased feelings of safety on the Internet. In summary, the awareness workshop had a positive impact on students' perception of online security, leading to a significant increase in their sense of safety.

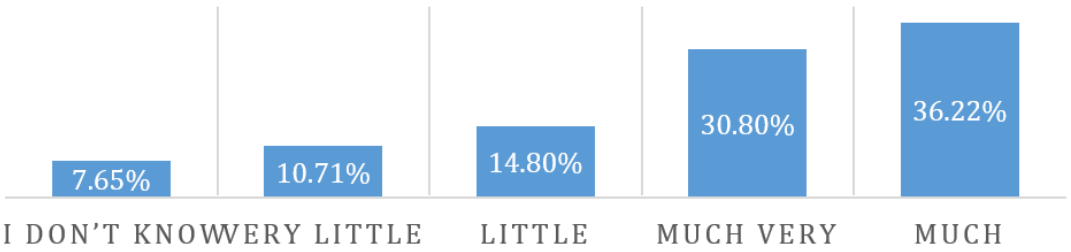

Figure 6: Perception of internet-based Learning (Post-Workshop)

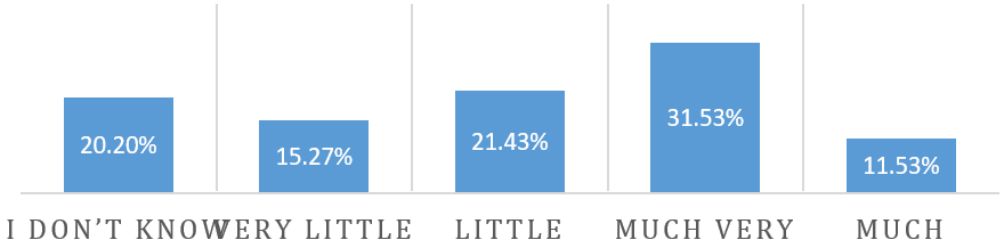

Figure 7: Perception of Internet for Studying

Interpretation of Figure-8, 9

The figure above illustrates that a considerable portion of the surveyed students do not use the internet for academic purposes. Surprisingly, even among the total participants, the majority of students (26.13%) have not reported using the internet for academic research, and 24.12% of the students claim that they have never downloaded academic materials from the web. Additionally, a relatively small number of students (8.04%) mentioned using the internet for educational purposes.

The workshop on internet safety and cybersecurity, combined with academic guidance and a certain level of technical knowledge sharing, has proven to be highly effective. The students' commitment to learning significantly increased post-workshop, and the figures show a substantial shift in their perceptions. Following the workshop, 46.31% of students claimed they were now engaged in a much higher volume of learning. Additionally, 37.31% of students reported more significant involvement in their studies, while 6.60% of students stated that they were less engaged. This shift underscores the vital role of workshops and the need for a balance between guidance, technological proficiency, and information dissemination in enhancing students' commitment to learning.

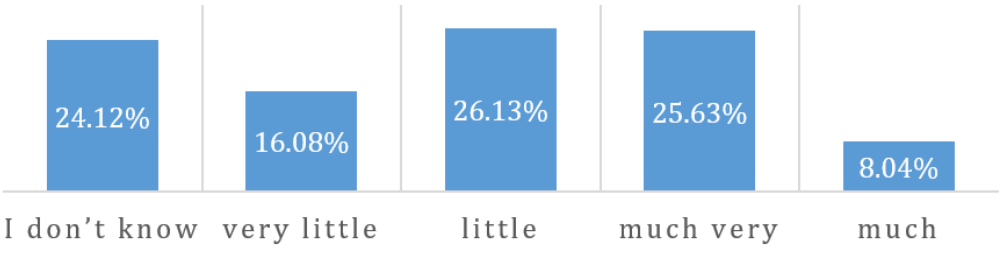

Figure 8: Internet use for acadamic purpose

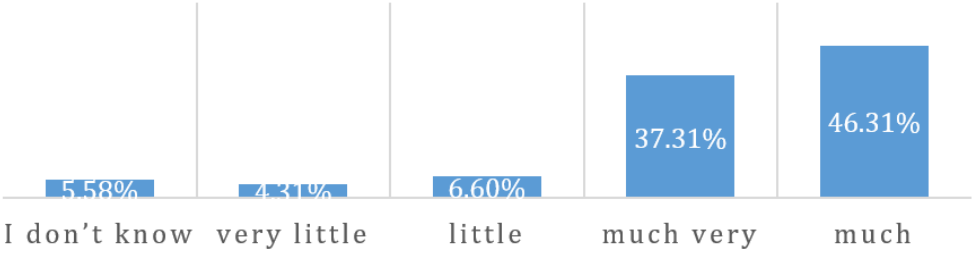

Figure 9: Knowledge of internet safety (after the workshop)

Interpretation of Figure-10

The figure below illustrates students' responses to questions concerning various activities related to internet use. Approximately 30% of the students claimed that they did not interact with unknown individuals online, while 21% indicated that they did not share their personal information with online contacts. Furthermore, 18% claimed that they did not disclose their passwords, and

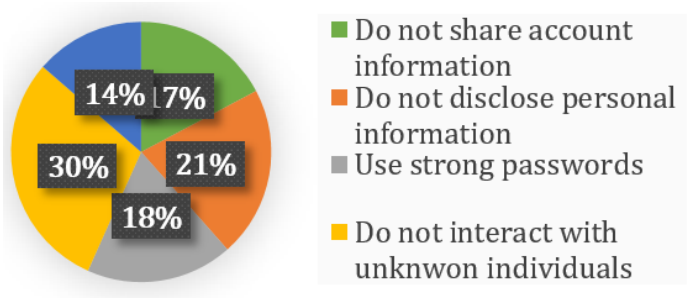

Figure 10: On Internet Use and Student Activities

17% stated that they did not share their account details. Additionally, 14% mentioned that they refrained from engaging in any academic activities on the internet.

Interpretation of Figure-11, 12

The findings from the figure below reveal the significance of using strong and secure passwords in online behavior. Approximately 67% of the students claim to use different and complex passwords for various accounts, highlighting a responsible approach to online security. However, 33% of the students admit to using easy-to-remember passwords, indicating the necessity for further education through workshops on the importance of robust password practices.

In the workshop, it was revealed that a significant 67% of the students utilize strong and complex passwords for their accounts. However, with the workshop's intervention, this number is expected to increase substantially, as 82% of students are now inclined to set strong passwords. On the other hand, the percentage of students who plan to change their passwords is noteworthy, with 33% aiming to do so, and 18% deciding to reset their passwords. This indicates a positive shift towards better password practices following the workshop.

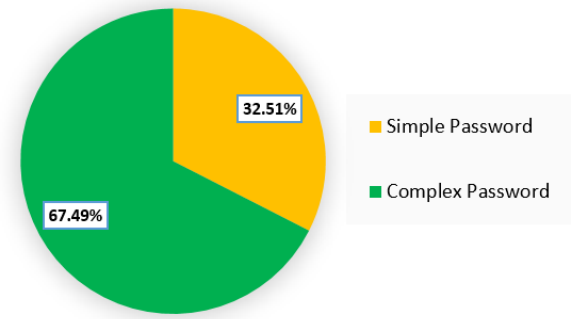

Figure 11: Types of Password Usage

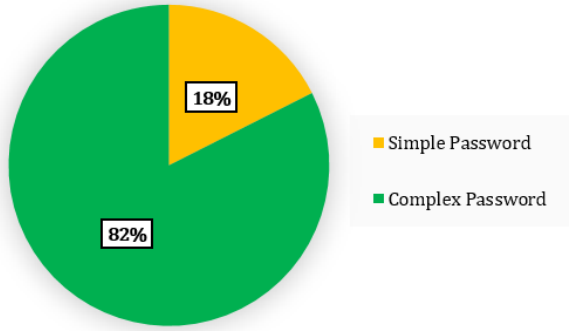

Figure 12: Types of Password Usage

Interpretation of Figure-13

In response to the question about internet censorship, the students' opinions varied significantly. A substantial portion, specifically 29.62% of the students, expressed that they had no concerns about internet censorship. However, 25.57% of the students believed that there is significant internet censorship, and 10.38% claimed that there is minimal censorship. It's worth noting that these figures significantly shifted after the workshop, particularly in the case of students who initially believed in minimal censorship.

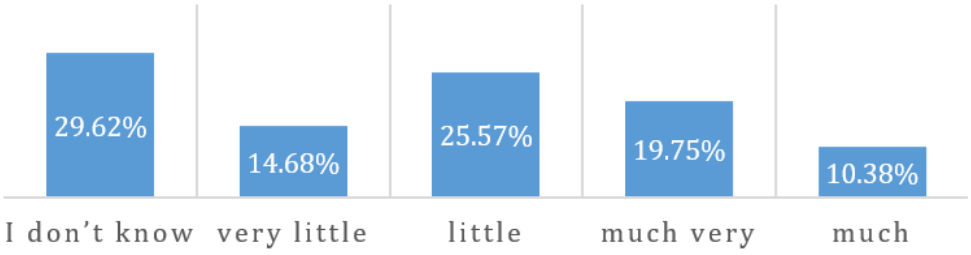

Figure 13: Regarding internet censorship

Interpretation of Figure-14

In response to the question about strategies for evading internet censorship, the students demonstrated varying opinions. A significant majority, specifically 53.77% of the students, believed that they were aware of strategies to evade censorship, whereas 24.68% indicated that they had little knowledge in this regard. Furthermore, 4.68% of students expressed knowledge of various advanced techniques for evading censorship, while 3.64% of the students provided no definitive response. It's important to note that these figures could change after attending the workshop.

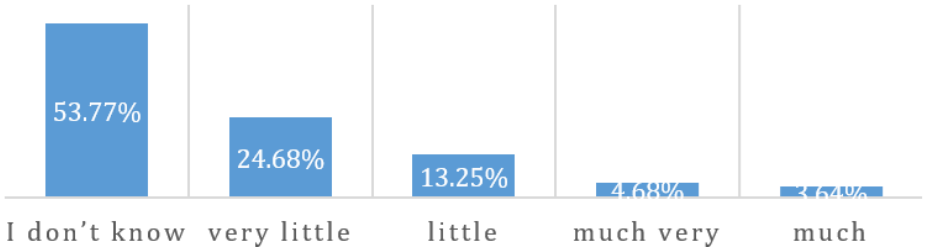

Figure 14: Internet Censorship Evation Strategies

Interpretation of Figure-15

When questioned about methods of online harassment, students presented various perspectives. Approximately 40% of the students believed they had not encountered online harassment, while 20% identified messaging apps as a common platform for such incidents. Moreover, 18% of the students mentioned Facebook as a channel for online harassment, and 16% cited mobile devices. In addition, a smaller portion, around 6%, acknowledged email-based harassment as well. It is worth noting that the lower percentage in email harassment might be attributed to its declining us.

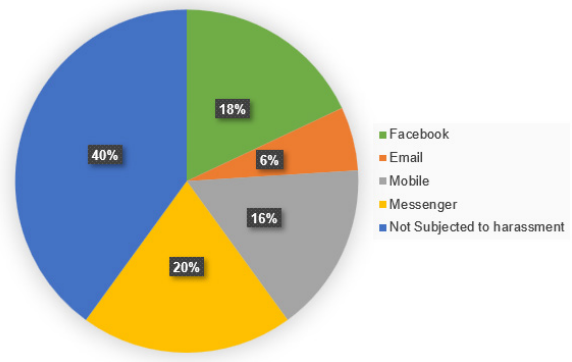

Figure 15: Methods of Online Harassment

Interpretation of Figure-16

The figure below provides insights into the diverse forms of online harassment and their prevalence among students. Impersonation or fake identity harassment was reported by a significant number of students, accounting for 40% of the respondents. Account hacking-related harassment affected 32% of students. Furthermore, 22% of students reported instances of image manipulation harassment. Less common forms of harassment, such as revealing personal secrets, were reported by 6% of the participants. These findings underscore the need for awareness and education regarding online safety and responsible behavior.

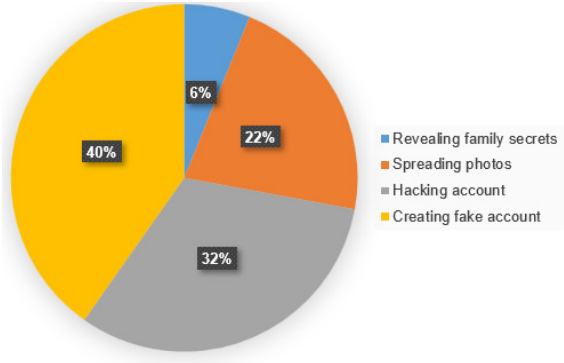

Figure 16: Types of online harassment

Interpretation of Figure-17

Internet abuse for various purposes and types of abuse occurs for different goals. The most significant The figure below illustrates various forms of internet abuse categorized by their purposes and objectives. The most prominent category, comprising approximately 76% of cases, is internet abuse aimed at harassing and causing harm to others. About 16% of cases are attributed to financial extortion, where individuals engage in financial demands. The dissemination of information, affecting various levels of victims, accounts for 4% of cases. Finally, around 4% of cases relate to sexual abuse on the internet, raising significant concerns. These findings emphasize the need for addressing these distinct forms of internet abuse and implementing preventive measures.

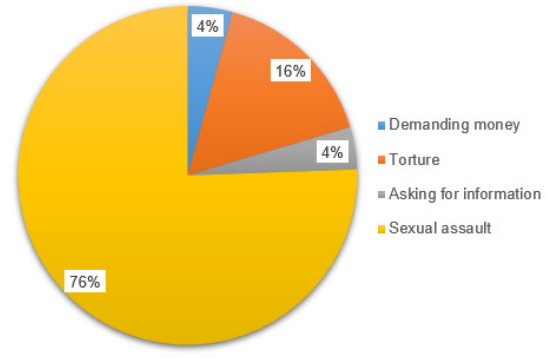

Figure 17: Purpose of internet bullying

Interpretation of Figure-18

The figure below highlights the importance of seeking

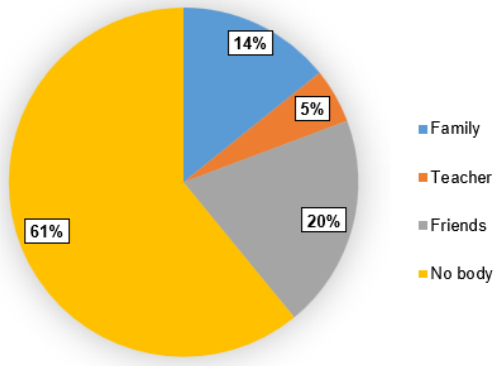

Figure 18: Advice on Internet addiction before workshop

advice on internet bullying, as it can affect anyone online. According to this survey, a significant percentage, approximately 20%, prefer to seek advice from their friends, while 14% turn to family members for guidance. In contrast, 61% mentioned that they do not seek advice from anyone. It's worth noting that these figures have been updated based on insights from a recent workshop, reflecting a more informed approach to addressing internet bullying.

Interpretation of Figure-19

Before the workshop, the knowledge of the students was extremely low and disappointing to the extent that they did not even understand the concept of cyberbullying. But when we gave an awareness workshop about cyber security, the awareness increased and there was a visible change in the survey data. In the survey, 42.49% of the students claimed to have a lot of knowledge and 34.72% of the students claimed to have a lot of knowledge. But

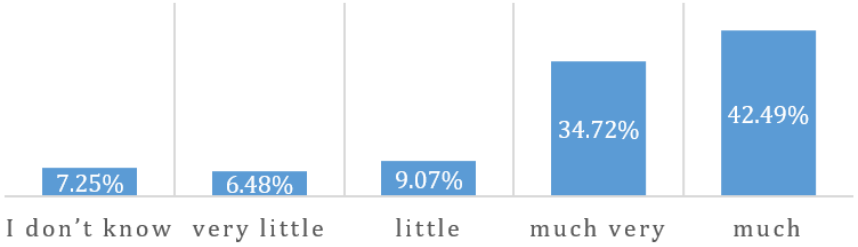

Figure 19: Knowledge of the Internet(after the workshop)

then 9.07% students claimed to have little knowledge.

Interpretation of Figure-20

The figure below illustrates the impact of counselling for internet bullying following the awareness workshop. Before the workshop, approximately 8% of students reported not seeking any counselling. However, after the awareness workshop, this percentage significantly decreased to 9%. Family consultation showed an increase from 20% to 29%, while teacher consultation rose from 5% to 23%. These changes indicate the positive influence of the awareness workshop in encouraging students to seek counselling and guidance when facing internet bullying issues.

Interpretation of Figure-21

Before the awareness workshop, the students had little to no knowledge of the significance of internet safety. However, through the awareness workshop, their understanding improved, and they recognized its importance. The survey data indicated a marked shift compared to the previous results. Specifically, 46.48% of students stated a high level of importance, while 6.16% of students considered it to be of lesser significance.

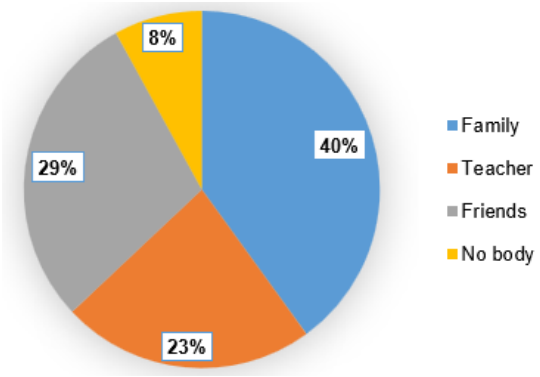

Figure 20: Advice on Internet addiction after the workshop

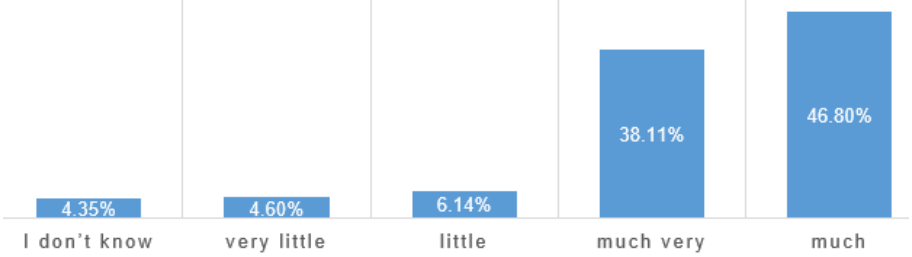

Figure 21: The Significance of Internet Safety

Verification of Recommended Solutions

The survey served as the proposed solution, and its effectiveness was assessed through feedback from school administrators, head teachers, and associate professors, as detailed in the evaluation report. Compliance of principals, head teachers and lecturers to give the workshop.

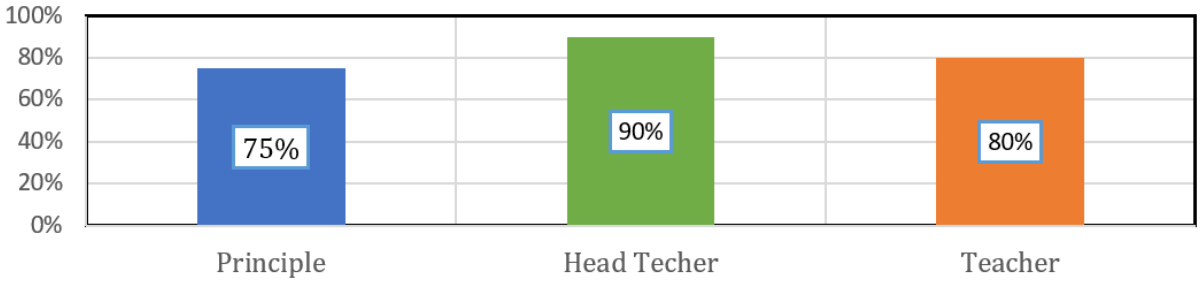

Figure 22: Compliance of principals, principals and teachers with video games

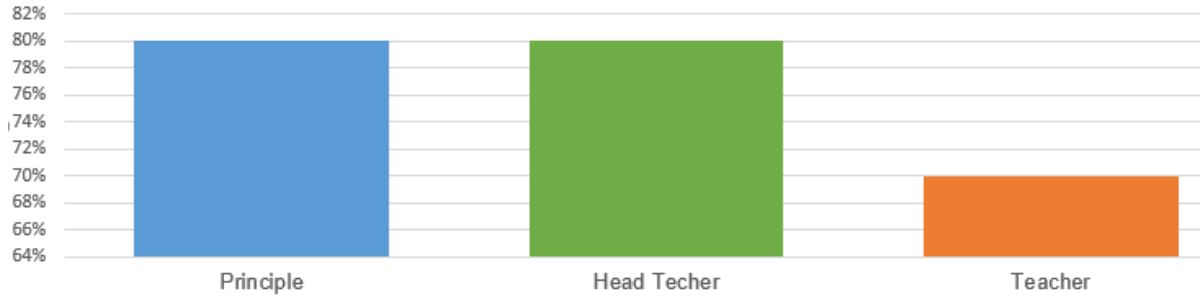

Figure 23: Compliance of principals, Head Teacher and Teachers with video games

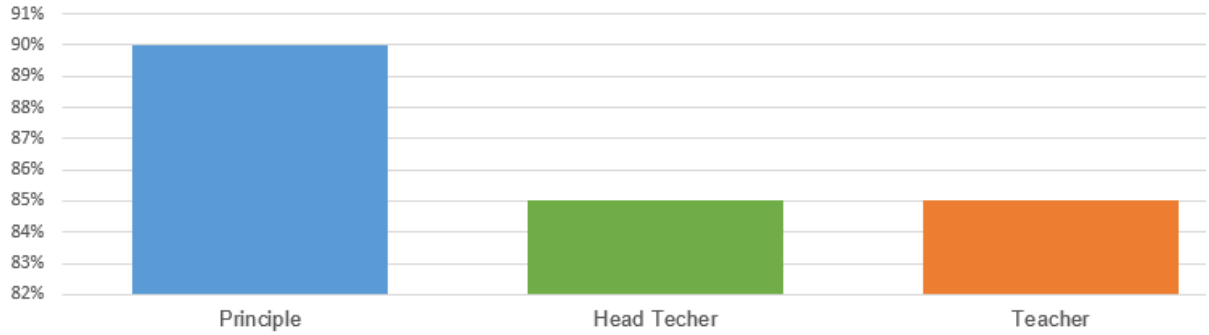

Figure 24: Agreement of principals, Head teachers and Teacher to add topics on cyber security in civics and computer textbooks

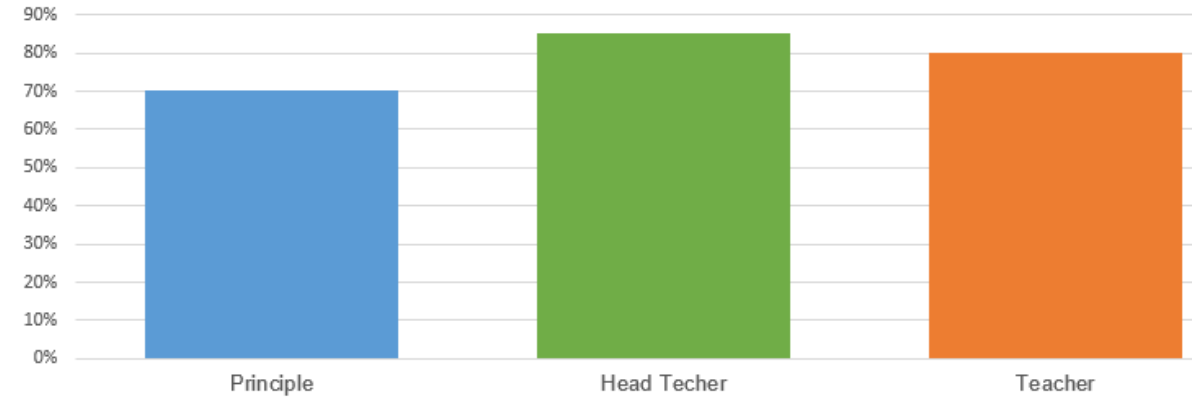

Figure 25: Agreement of principals, Head teachers andTeacher to add a subject on cyber security to the academic curriculum.

The Best Solution

Interpretation of Figure-26

The comprehensive analysis of the four proposed solutions indicates that adding topics about cybersecurity to civics and computer textbooks emerges as the most favored option among the surveyed stakeholders. With an impressive overall average agreement of 78.30%, this solution outperforms the alternatives. The proposal to add a subject on cybersecurity to the academic curriculum follows closely behind, garnering substantial support with an average agreement of 86.60%. Workshops on cybersecurity education also demonstrate strong backing, with an average agreement of 81.60%, emphasizing their efficacy in engaging participants. The use of video games for cybersecurity awareness, while still receiving positive feedback at 76.60%, ranks slightly lower than the other

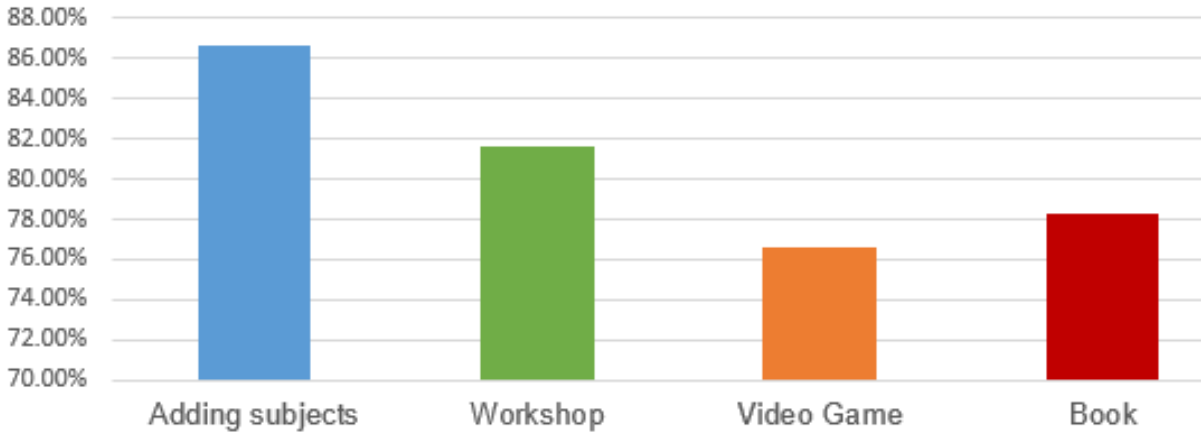

Figure 26: A summary of four Optimal Strategies for Enhancing Cybersecurity Education

solutions. In conclusion, the consensus suggests that integrating cybersecurity topics into civics and computer textbooks stands out as the most promising and widely accepted approach, warranting further consideration and potential implementation in the academic setting.

DISCUSSION

In this research exploration of the imperative realm of enhancing internet safety and cybersecurity awareness among secondary and high school students, particularly in Badakhshan Province, Afghanistan, our research delves into a multifaceted landscape. As our digital age unfolds, the ubiquity of the internet demands an adept youth equipped with skills for secure online navigation. The study underscores the global trend of integrating cybersecurity education into curricula while addressing the unique challenges and opportunities in Afghanistan.
findings illuminate the prevalence of cyber threats, emphasizing the need for proactive measures to ensure students are well-prepared. The lack of cybersecurity awareness exposes students to risks like cyberbullying and online scams, necessitating immediate action. This case study serves as a crucial examination of existing practices, strategies, and potential areas of improvement in enhancing internet safety and cybersecurity awareness. It advocates for a holistic approach encompassing technical skills, ethical values, and responsible digital citizenship. The significance of our research lies in bridging the gap between the education sector and the cybersecurity domain. By proposing practical solutions and offering a blueprint for implementation, our study contributes to academic knowledge and serves as a reference for policymakers, educators, and institutions. Through a comprehensive methodology involving both quantitative and qualitative analyses, we provide valuable insights into the internet behavior and cybersecurity awareness of the youth in Badakhshan Province. In essence, our commitment to cybersecurity education extends beyond protecting students; it aims to empower them to navigate the digital world responsibly and ethically, fostering a safer, more informed society.

CONCLUSIONS

In conclusion, as we tread the path of our digital age, the need for cybersecurity education among our youth becomes ever more apparent. The internet, a vast and influential tool, offers opportunities for growth and enlightenment, but it also exposes our students to various digital dangers. These include cyberbullying, privacy infringements, and security threats, all of which are real concerns that affect our students. Our research, cantered in the heart of Badakhshan Province, Afghanistan, has brought to light the positive impact of cybersecurity education. It has underscored the urgent requirement for digital literacy and online safety principles to be instilled in students across different age groups and academic fields. Additionally, it has highlighted the crucial role of parental engagement in nurturing responsible digital behaviors that encompass aspects like privacy, security, and copyright. Through a meticulous research process involving both quantitative and qualitative analysis, we have gained valuable insights into the online behavior and cybersecurity awareness of the youth in this region. We've come to understand their online activities and their level of digital literacy. This knowledge forms a solid foundation for the integration of cybersecurity education into school curricula, an initiative aimed at empowering students to navigate the digital landscape with confidence and ethical awareness. By doing so, we ensure their online privacy and security and tap into the internet's full potential as a resource for education. In summary, our dedication to cybersecurity education isn't just about protecting our students; it's about preparing them to be responsible, knowledgeable, and well-informed digital citizens. It's about fostering a safer, more responsible, and knowledge-driven society. As we move forward, let's remember that the journey to a safer digital world begins with a single click, and together, we can make a profound impact. In essence, we reiterate our strong call to integrate cybersecurity education into school curricula, nurturing a generation of responsible digital citizens who will confidently and ethically navigate the digital landscape. It's a commitment to their security, their future, and the brighter horizons of an interconnected digital world.

Acknowledgement

I extend my heartfelt appreciation to Mr. Musawer Hakimi and other colleagues for their invaluable support in the completion of this research paper. Their assistance in writing, data analysis through SPSS, and data collection was instrumental in bringing this study to fruition. Their expertise and dedication significantly enhanced the quality of this work, and I am deeply grateful for his contributions. In addition, I would like to express my gratitude to my family and friends who have been a continuous source of support and encouragement throughout this research journey. Their unwavering belief in my capabilities and their understanding of the demands of this endeavor have been a constant source of motivation and inspiration. This paper was made possible with the collaborative efforts of those mentioned above. Their contributions have enriched the quality and depth of this research.

REFERENCES

Adams, R., & Brown, T. (2018). Preparing the Next Generation: The Role of Educational Institutions in Cybersecurity. *International Journal of Cybersecurity Education, 6*(1), 45-61.

Anderson, M., & Milfont, J. (2017). Collaborative Efforts in Cybersecurity Education: Involving Parents in the Process. *Journal of Educational Collaboration, 10*(1), 42-56.

Australian Government Department of Education. (2021). National Cybersecurity Education Initiatives. Retrieved from https://www.education.gov.au/

Bornaa, C. S., Abugri, M. A., & Iddrisu, A. B. (2023). Comparative Study of Traditional Face-to-Face and E-Learning Modes of Teaching Senior High School Geometry. *American Journal of Education and Technology, 2*(2), 10-14.

Canadian Centre for Cyber Security. (2018). The Role of Cybersecurity Education in Ensuring a Secure Digital Future. Retrieved from https://cyber.gc.ca/

Colette, B. (2018). *Qualitative and Quantitative Data Analysis Methods*. Retrieved from https://humansofdata.atlan.com/2018/09/qualitative-quantitative-data-analysis-methods/

Cybersecurity & Infrastructure Security Agency. (2019). National Strategy for Cybersecurity Education. Retrieved from https://www.cisa.gov/

Duggan, M. (2020). The Impact of Cybersecurity Education on Digital Citizenship. *Journal of Educational Technology Research, 11*(4), 149-165.

European Union Agency for Cybersecurity. (2021). National Initiatives for Cybersecurity Education Across Europe. Retrieved from https://www.enisa.europa.eu/

Express Computer. (2020). Notorious Cyber Security Attacks in India to Date. Retrieved from https://www.expresscomputer.in/security/notorious-cyber-security-attacks-in-india-to-date/

Government of the United Kingdom. (2020). National Cybersecurity Education Initiatives. Retrieved from https://www.gov.uk/cyber-security-education-initiatives

Hakimi, M., Fazil, A. W., Khaliqyar, K. Q., Quchi, M. M., & Sajid, S. (2024). Evaluating The Impact of E-Learning on Girl's Education in Afghanistan: A Case study of Samangan University. *International Journal of Multidisciplinary Approach Research and Science, 2*(01), 107-120.

International Society for Technology in Education. (ISTE). (2019). Cybersecurity Education Standards for Students. Retrieved from https://www.iste.org/

Japan Ministry of Education. (2017). Integrating Cybersecurity into the Japanese Educational System. Retrieved from https://www.mext.go.jp/en/

Johnson, L., *et al.* (2019). Building Cybersecurity Awareness Among Young Learners: A Comprehensive Framework. *Journal of Information Security Education, 14*(3), 215-231.

Jones, S., & Brown, E. (2020). The Necessity of Comprehensive Cybersecurity Education in a Digital World. *International Journal of Information Security, 8*(3), 211-225.

Li, K., *et al.* (2019). Fostering a Safer Digital Environment for Students through Cybersecurity Education. *Journal of Digital Education, 12*(4), 155-168.

Livingstone, S., & Bulger, M. (2014). Promoting Digital Citizenship Through Cybersecurity Education. *International Journal of Digital Ethics, 3*(2), 79-93.

McLeod, S. (2018). Questionnaires. Retrieved from https://www.simplypsychology.org/questionnaires.html

Ministry of Education. (2018). *School Books*. Kabul: Ministry of Education.

National Cyber Security Policy. (2013). Cybersecurity Education at the National Level. Retrieved from https://www.cybersecuritypolicy.org

National Institute of Standards and Technology. (NIST). (2020). Cybersecurity Framework for Schools and Educational Institutions. Retrieved from https://www.nist.gov/

Natividad, R. J. P., & Abrogena, L. G. (2023). Availability of Technological Learning Applications and Tools, Science Teachers' Levels of Use of Online Teaching, and Their Stages of Concerns. *American Journal of Multidisciplinary Research and Innovation, 2*(3), 97-109.

Norton, A., *et al.* (2017). Parents as Partners: Strengthening Cybersecurity Education Through Family Involvement. *Cybersecurity Journal, 5*(2), 87-102.

Orr, J. (2019). Case Studies. Retrieved from https://www.cshub.com/case-studies

Rodriguez, M., *et al.* (2016). Fostering Responsible Digital Citizenship through Cybersecurity Education. *Journal of Digital Learning, 8*(3), 137-152.

Sethunathan, B. (2020). 5 Key Strategies for Creating a Cyber Awareness Program. Retrieved from https://www.softwareone.com/en-za/blog/articles/2020/03/02/5-key-strategies-for-creating-a-

cyber-awareness-program

Smith, J., *et al.* (2018). Imparting Digital Literacy and Cybersecurity Skills to Young Learners. *Journal of Educational Technology, 14*(2), 87-101.

United Nations Educational, Scientific and Cultural Organization. (UNESCO). (2018). Digital Literacy and Cybersecurity: A Global Perspective. Retrieved from https://unesdoc.unesco.org/

Valcheva, S. (2020). Types of Graphs and Charts. Retrieved from http://www.intellspot.com/types-graphs-charts/