Submitted: 19 August 2024 | Accepted: 20 October 2024 | Published: 21 October 2024

RESEARCH PAPER

Volume 3 Issue 1 (2024), E ISSN- 2987-968X

Journal of Social and Humanities

https://jurnal.tintaemas.id/index.php/JSH/index

Examining the Impact of Cyberattacks on Women's Digital Security: Challenges and Solutions

Freshtah Fazel *[,1], **Sonia Arsalan** [2], **Madina Ahmadi** [3], **Zainab Bahaduri** [4], **Tamanna Quraishi** [5]

[1] Theology Faculty, Herat University, Afganistan, fareshtahfazl11@gmail.com

[2] Pharmacy Faculty, Rahnaward Private University, Balkh, **Afghanistan**, sonyaarsalan1@gmaill.com

[3] Faculty of Engineering, Kabul University, **Afghanistan**, madina.ahmadi4321@gmail.com

[4] BiBi Sarah School, Kabul, **Afghanistan**, zainabhamtab@gmail.com

[5] Computer Science Faculty, University of the People, **USA**, tamannaquraishi259@gmail.com

Abstract

This study investigates the challenges faced by women in maintaining digital security amid rising cyberattacks and examines the effectiveness of gender-sensitive policies and educational programs aimed at improving women's cybersecurity. As cyber threats increasingly target women, understanding their unique vulnerabilities and the role of specific protective measures is crucial. The research utilizes a quantitative approach with a structured questionnaire distributed to 150 participants across four faculties of an online university, including Medical, Economics, Education, and Computer Science. The data collected were analyzed to assess perceptions of digital security challenges, the effectiveness of gender-sensitive policies, and the importance of educational programs in enhancing women's participation in cybersecurity. Results indicate that while gender-sensitive policies are viewed as somewhat effective, there is significant support for targeted educational programs to increase women's involvement in cybersecurity. The findings highlight the need for more refined policies and better educational initiatives to address women's unique digital security needs effectively. The study underscores the importance of implementing comprehensive strategies to improve women's cybersecurity and promote their active participation in the sector.

Keywords: Digital Security, Cybersecurity, Gender-sensitive Policies, Educational Programs, Women's Participation.

1. INTRODUCTION

The increasing prevalence of cyberattacks presents a significant threat to digital security worldwide. However, women, in particular, face unique challenges when navigating the digital landscape, as they are disproportionately affected by cyber threats such as online harassment, identity theft, and privacy violations. Cyberattacks against women not only compromise their personal information but also contribute to a larger systemic issue of gender inequality in the cybersecurity domain [1]. This introduction explores the specific ways in which women are targeted by cyberattacks, the challenges they face in maintaining digital security, and potential solutions to address these issues.

As digital spaces continue to grow and evolve, so do the opportunities for women to engage with technology in professional, educational, and social contexts. However, the expansion of digital engagement has also exposed women to a range of cyber threats, from revenge porn and doxing to cyberstalking and online harassment [2]. These attacks are often gender-specific, driven by underlying societal issues such as sexism and misogyny, which further complicate efforts to ensure the digital safety of women. In many cases, victims of cyberattacks face additional psychological trauma, emotional distress, and reputational damage, which can have lasting effects on their personal and professional lives [3].

Despite the severity of these threats, there remains a significant gap in cybersecurity policies and practices designed to protect women. Research highlights the underrepresentation of women in the cybersecurity sector, which may contribute to the lack of gender-sensitive approaches to addressing online threats [4]. Women's participation in cybersecurity is critical not only for increasing diversity in the field but also for ensuring that cybersecurity solutions take into account the unique vulnerabilities women face online [5]. Without targeted policies and practices, many women remain vulnerable to attacks that exploit both technical and social weaknesses.

Addressing these challenges requires a multifaceted approach. This includes improving

* **Correspondence Address**
Theology Faculty, Herat University, **Afganistan**, fareshtahfazl11@gmail.com

education and awareness about cybersecurity risks among women, enhancing legal frameworks to combat cybercrime, and encouraging greater female participation in the cybersecurity field [6]. Furthermore, technology companies and policymakers must prioritize the development of tools and policies that specifically address the digital security needs of women, ensuring that they can navigate online spaces without fear of attack [7].

This study aims to identify the primary challenges women face in protecting their digital security from cyberattacks, analyze the effectiveness of existing cybersecurity policies in addressing these challenges, and propose actionable strategies to enhance women's participation in the cybersecurity sector. By focusing on these aspects, the research seeks to contribute to the development of more inclusive cybersecurity practices that empower women and promote their safety online.

Cyberattacks disproportionately target women, exposing them to a range of gender-specific threats such as online harassment, cyberstalking, identity theft, and privacy breaches. Despite the growing recognition of digital security concerns, current cybersecurity measures often fail to account for the unique vulnerabilities faced by women. The lack of gender-sensitive policies and inadequate representation of women in the cybersecurity workforce exacerbates the issue, leaving many women without effective tools or legal protection against cyber threats. Furthermore, the psychological and emotional impact of cyberattacks on women is frequently overlooked, resulting in underreported cases and insufficient support for victims. This research aims to address these gaps by examining the challenges women face in maintaining digital security and proposing practical solutions, including enhanced legal frameworks, improved digital literacy, and the development of gender-specific cybersecurity measures to better protect women in the digital age.

The issue of cybersecurity for women has gained increased attention as digital spaces have become essential in modern life. However, women are disproportionately targeted by cyber threats such as online harassment, identity theft, and privacy breaches, highlighting significant gaps in cybersecurity measures. According to [1-2], the underrepresentation of women in the cybersecurity sector has hindered the development of gender-sensitive solutions to these issues, exacerbating the vulnerabilities women face. [3-4] emphasizes the urgent need to increase the participation of women in cybersecurity, which would contribute to more inclusive and effective solutions.

Gender-specific cyberattacks, driven by societal norms that perpetuate misogyny, often exploit both technical and social vulnerabilities. [5] emphasize that cyberattacks targeting women are often socially driven, necessitating a deeper understanding of gender in cybersecurity frameworks. Peacock and Irons [6-7] further argue that cybersecurity policies fail to account for the gendered nature of these threats, as women are often subjected to unique forms of online harassment, including cyberstalking and revenge pornography. These forms of harassment have significant psychological and emotional effects, yet current cybersecurity strategies rarely address them directly [8-9].

Additionally, the absence of gender-specific policies in cybersecurity perpetuates the issue. [10-11] argue that the cybersecurity behaviors of men and women differ, and the lack of recognition of these differences leaves women vulnerable to attacks. [12] emphasizes the importance of women's participation in cybersecurity to ensure policies adequately address gender-specific threats. By increasing the number of women in leadership positions, more comprehensive cybersecurity strategies could be developed, providing women with better protection in the digital realm [13].

Cybersecurity education plays a crucial role in protecting women from digital threats. [13] argue that cybersecurity education should be considered as fundamental as basic literacy skills, particularly for women. Women must be equipped with the knowledge and skills necessary to protect themselves in the digital world. [14] suggest that early intervention through cybersecurity awareness programs in educational institutions can significantly improve women's ability to navigate the digital landscape safely.

In Afghanistan, where social engineering attacks disproportionately affect women, [15-16] have examined strategies to strengthen women's resilience to these attacks. Their findings indicate that gender-sensitive cybersecurity measures can significantly reduce the risks faced by women, emphasizing the importance of targeted interventions. This view is echoed by [17], who highlight the significance of gender equality in the cybersecurity sector, suggesting that empowering women through education and professional opportunities can lead to more robust cybersecurity frameworks.

In summary, the literature underscores the critical need for gender-sensitive cybersecurity policies and education. Women face unique cyber threats that current policies do not adequately address, and the lack of female representation in the sector perpetuates this issue. Enhancing cybersecurity education and increasing women's participation in the cybersecurity

field are essential steps in developing more comprehensive and inclusive strategies to safeguard women online.

2. METHOD

Research Design

This study employs a quantitative research design to investigate women's digital security challenges and opportunities. A structured questionnaire with Likert-scale questions was used to collect data on participants' perceptions of cybersecurity issues, the effectiveness of gender-sensitive policies, and the impact of educational programs. This design allows for a systematic analysis of the variables and facilitates comparison across different groups.

Population and Sampling

The study targeted students from four faculties at an online university, totaling 150 participants. The population was divided as follows:

- **Medical Faculty**: 40 participants, aged 20-25 years.
- **Economics Faculty**: 40 participants, aged 18-24 years.
- **Education Faculty**: 40 participants, aged 19-24 years.
- **Computer Science Faculty**: 30 participants, aged 20-24 years.

A stratified random sampling method was employed to ensure representation from each faculty. This approach provided a balanced view of the challenges and perceptions across different academic disciplines and age groups.

Data Collection

Data were collected using a self-administered online questionnaire. The questionnaire included multiple-choice questions with Likert scale responses, focusing on:

1. Perceptions of unique challenges women face in digital security.
2. Views on the effectiveness of gender-sensitive cybersecurity policies.
3. Opinions on the importance of educational programs in increasing women's participation in cybersecurity.

Participants were selected randomly from each faculty to ensure a representative sample. The online format facilitated broad reach and convenience for participants.

Data Analysis

The collected data were analyzed using descriptive methods. Frequencies and percentages were computed to summarize participants' responses to each question. Statistical tools such Excel software were used for data analysis to ensure accuracy and reliability. The findings were then interpreted to draw conclusions about the effectiveness of current strategies and identify areas for improvement in enhancing women's digital security.

3. RESULT AND DISCUSSION

Demographic Distribution of Participants

The results section presents a detailed analysis of participants' perceptions regarding digital security challenges, the effectiveness of gender-sensitive policies, and the importance of targeted educational programs in enhancing women's involvement in the cybersecurity sector. The findings provide insights into the current state of women's cybersecurity protection and participation, highlighting areas for improvement and further research.

Table 1 Demographic Distribution of Participants by Faculty and Age Range

Faculty	Number of Participants	Age Range (Years)
Medical	40	20-25
Economics	40	18-24
Education	40	19-24
Computer Science	30	20-24
Total	150	-

The demographic table reflects a well-distributed population of 150 women from four different faculties at the online university. The majority of participants are aged between 18-25 years, indicating a relatively young population, which aligns with typical university demographics. The largest groups come from the Medical, Economics, and Education faculties, each contributing 40 participants, while the Computer Science faculty has a slightly smaller representation with 30 participants. This distribution ensures a balanced approach when examining the perspectives of women from diverse academic fields, potentially offering insights into how faculty-specific challenges impact cybersecurity awareness and digital safety among women. The age range provides a focused view on the younger generation's engagement with cybersecurity issues.

Demographic of Summarizes Responden Answers

The **Figure 1** summarizes the responses of 150 participants regarding the perception that women face unique challenges in maintaining digital security compared to men. A significant portion of participants (33.33%) agree, and an additional 26.67% strongly agree, indicating that the majority recognize the distinct challenges women encounter in digital security. Conversely, only a small fraction of participants (6.67%) strongly disagree, suggesting a

consensus on the existence of these challenges. The neutral responses (20.00%) may reflect uncertainty or a lack of personal experience with the issue. Overall, the data suggests that there is considerable acknowledgment of gender-specific digital security challenges among the participants.

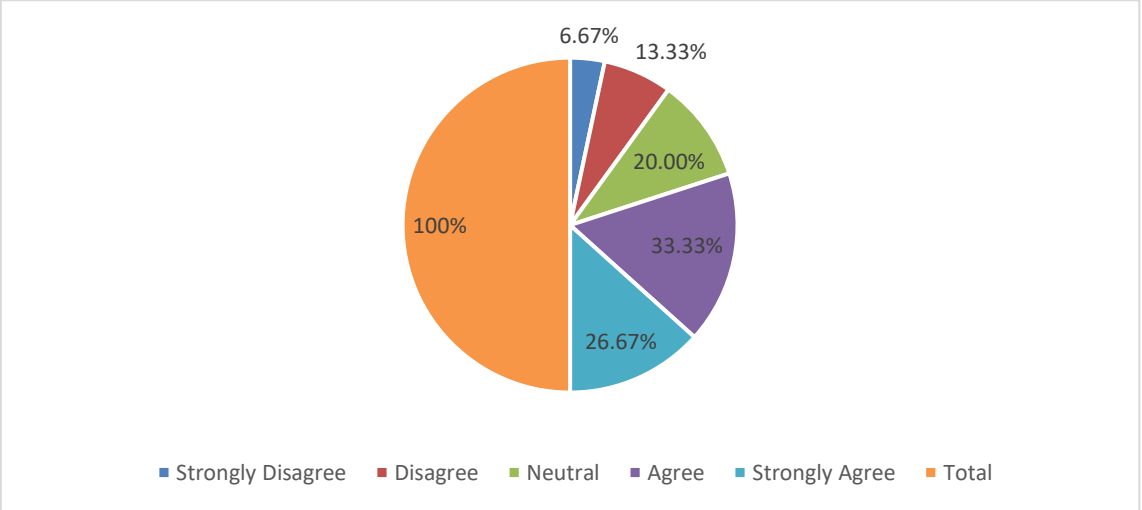

Figure 1 Participants' Perceptions on Unique Challenges Women Face in Maintaining Digital Security Compared to Men

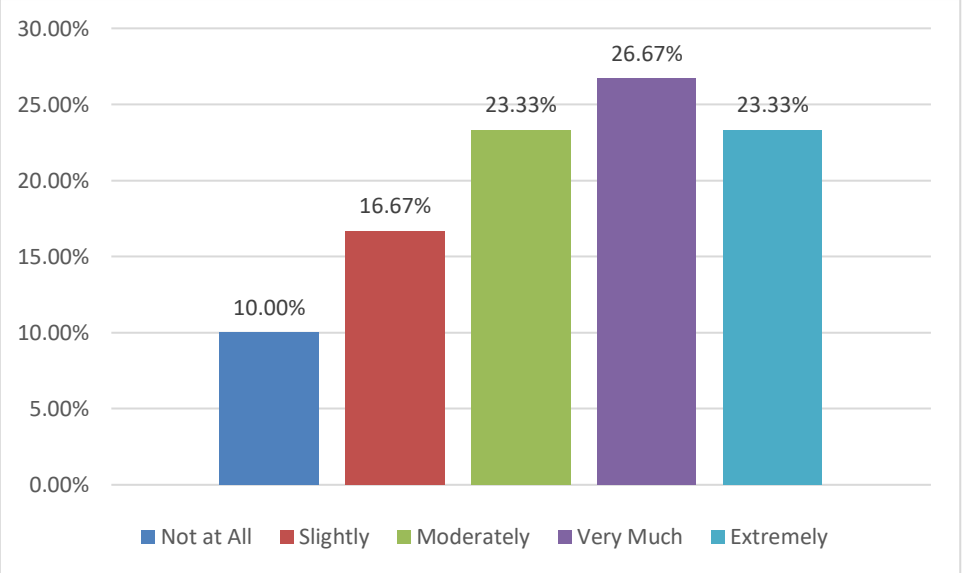

Figure 2 Participants' Views on the Impact of Increasing Cyberattacks on Women's Digital Security

The **Figure 2** presents the distribution of participants' beliefs regarding the impact of increasing cyberattacks on women's digital security. A substantial proportion of respondents (26.67%) believe that cyberattacks have impacted women's digital security "Very Much," and an additional 23.33% perceive the impact as "Extremely." This indicates a strong sentiment that cyberattacks are significantly affecting women's digital security. Conversely, a smaller percentage of participants (10.00%) feel that the impact is "Not at All," suggesting that some do not view the issue as severe. The "Moderately" (23.33%) and "Slightly" (16.67%) responses reflect a range of perspectives, with moderate to slight recognition of the problem. Overall, the data indicates a consensus that increasing cyberattacks have a considerable impact on women's digital security.

The **Figure 3** illustrates participants' views on the effectiveness of gender-sensitive policies in enhancing cybersecurity protections for women. A significant number of respondents (29.33%) consider these policies "Very Effective," and another 24.00% view them as "Extremely Effective," highlighting a strong belief in the positive impact of such policies. In contrast, only 8.00% find them "Not Effective," suggesting that while a small minority see little value in these policies, most recognize their benefits. The "Moderately Effective" category (24.00%) indicates that there is also a considerable number of participants who acknowledge some level of effectiveness, but not to an exceptional degree. Overall, the responses suggest that gender-sensitive policies are generally regarded as a valuable tool for improving cybersecurity protections

for women, though there is room for further enhancement and evaluation.

The above **Figure 4** summarizes participants' perceptions regarding whether existing cybersecurity policies adequately address women's specific needs. A significant portion of participants are "Neutral" (26.67%) or "Agree" (26.67%) with the adequacy of these policies, indicating a mixed yet generally positive view. However, 12.00% "Strongly Disagree" and 20.00% "Disagree," reflecting a notable proportion who believe the policies fall short in addressing women's needs. Conversely, only 14.67% "Strongly Agree," suggesting that while there is some recognition of the effectiveness of current policies, many feel that improvements are necessary. Overall, the data reveals a general consensus that while there is some effectiveness in current policies, there is substantial room for enhancement to better meet the specific needs of women in cybersecurity.

Figure 5 shows participants' views on the importance of increasing women's participation in the cybersecurity sector to address women's digital vulnerabilities. A significant majority of respondents view it as "Very Important" (32.00%) or "Extremely Important" (32.00%), indicating strong agreement on the crucial role that enhanced female representation plays in addressing digital vulnerabilities. Only a small percentage consider it "Not Important" (5.33%), reflecting that most recognize the significance of this issue.

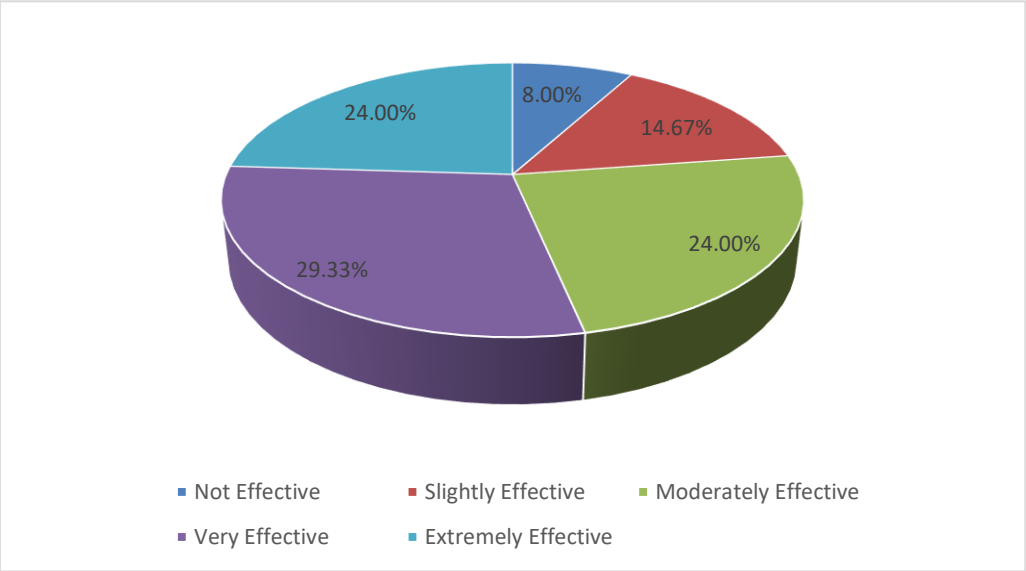

Figure 3 Participants' Opinions on the Effectiveness of Gender-Sensitive Policies in Improving Cybersecurity Protections for Women

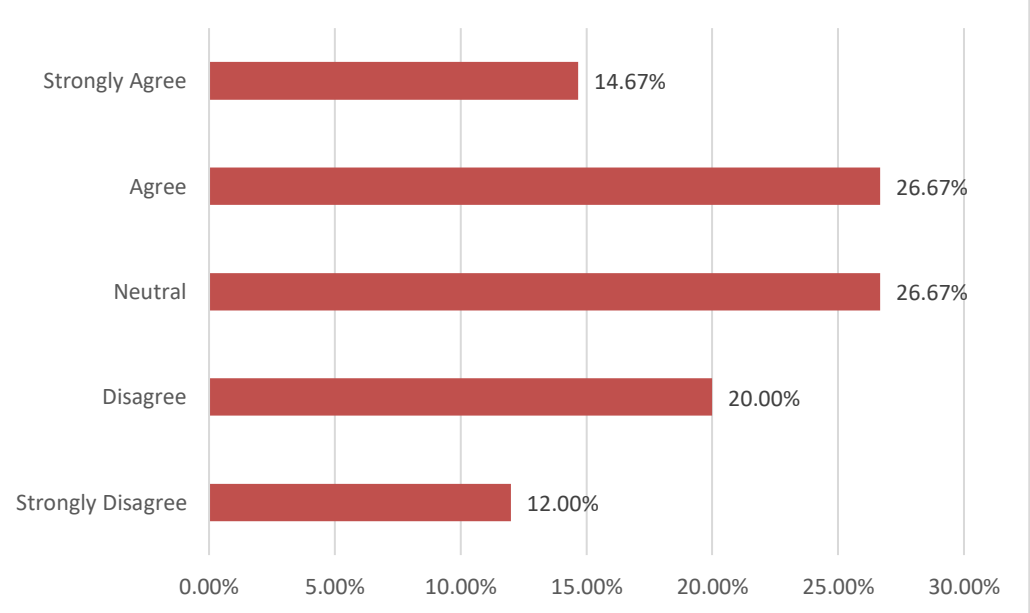

Figure 4 Participants' Agreement on the Adequacy of Existing Cybersecurity Policies for Addressing Women's Specific Needs

"Slightly Important" (12.00%) and "Moderately Important" (18.67%) responses suggest some variation in perceived importance, but overall, the data highlights a consensus on the substantial impact that increased participation can have on improving digital security for women.

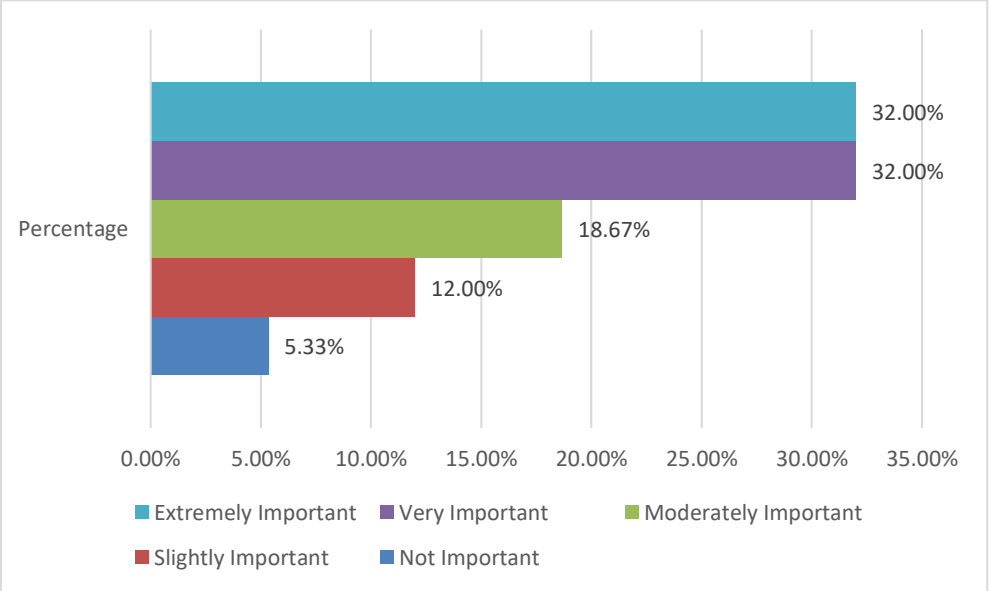

Figure 5 Importance of Increasing Women's Participation in the Cybersecurity Sector for Addressing Women's Digital Vulnerabilities

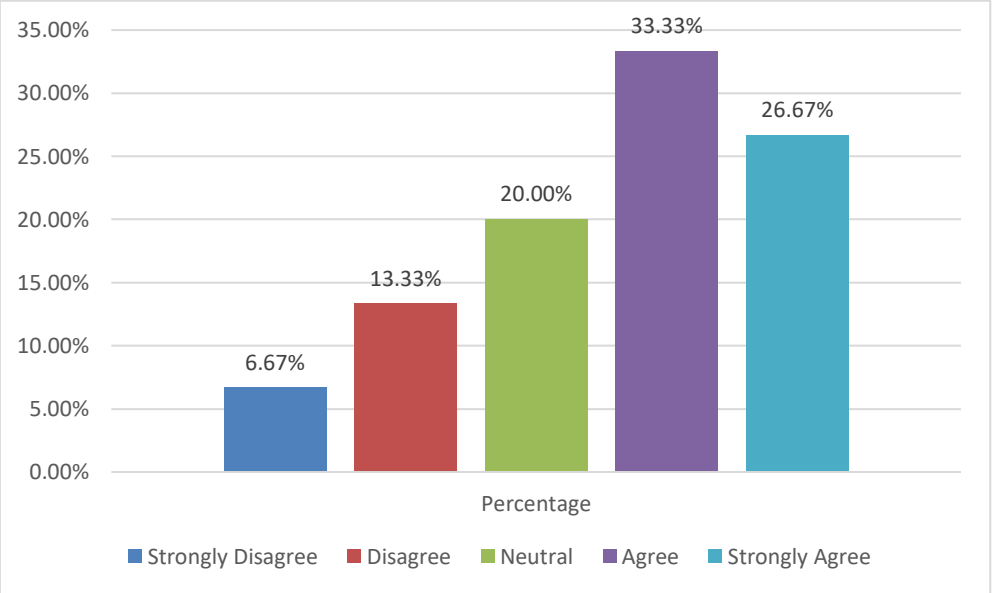

Figure 6 Agreement on the Impact of Targeted Educational Programs for Women on Enhancing Their Involvement in the Cybersecurity Sector

Figure 6 illustrates participants' opinions on whether targeted educational programs for women can enhance their involvement in the cybersecurity sector. A notable proportion of respondents "Agree" (33.33%) or "Strongly Agree" (26.67%) with the effectiveness of such programs, indicating a strong belief in the positive impact of educational initiatives. Only 6.67% "Strongly Disagree" and 13.33% "Disagree," suggesting a minority view on the ineffectiveness of targeted programs. The "Neutral" responses (20.00%) reflect some uncertainty or lack of personal experience with such programs. Overall, the data indicates broad support for the idea that specialized educational programs are beneficial in promoting women's participation in cybersecurity, though there remains some diversity in opinion.

Discussion

The findings of this study provide valuable insights into the challenges and opportunities related to women's cybersecurity. The results reveal a significant concern about the unique digital security challenges faced by women, as well as the perceived

effectiveness of gender-sensitive policies and targeted educational programs in addressing these challenges. The data indicates that a considerable majority of participant's view increasing cyberattacks as having a substantial impact on women's digital security. This aligns with existing literature, which highlights that women are disproportionately affected by cybersecurity threats due to a range of factors, including targeted attacks and cyberstalking [1], [2]. The high percentage of respondents who acknowledge the significant impact of cyberattacks underscores the urgent need for more robust cybersecurity measures and tailored protections for women.

In terms of gender-sensitive policies, the study finds a generally positive but mixed response. While a notable portion of participants consider these policies "Very Effective" or "Extremely Effective," a significant minority view them as "Not Effective" or "Slightly Effective." This reflects a broader debate in the field regarding the adequacy of current policies in addressing the specific needs of women [3,4], [18,19]. The mixed responses suggest that while progress has been made, there is still a need for more comprehensive and targeted policy development.

The findings regarding targeted educational programs for women reveal strong support for their role in enhancing participation in the cybersecurity sector. A majority of respondents agree that such programs are crucial for improving women's involvement and addressing digital vulnerabilities. This is consistent with research emphasizing the importance of educational initiatives in bridging the gender gap in cybersecurity and fostering greater female participation [5], [6]. The strong endorsement of educational programs suggests that investment in these initiatives could significantly contribute to increasing the number of women in cybersecurity roles.

However, the study also highlights areas where further research is needed. For instance, the varying perceptions of policy effectiveness and the need for more detailed studies on the impact of educational programs suggest that ongoing evaluation and refinement of strategies are essential. Future research should focus on developing and accessing new interventions and policies that more effectively address the unique needs of women in cybersecurity [7-9], [19-21].

Overall, the study emphasizes the importance of continuing efforts to improve digital security for women through targeted policies, educational programs, and increased awareness of their specific challenges. Addressing these issues is crucial for creating a more secure and inclusive digital environment.

4. CONCLUSION

This study provides a comprehensive overview of the challenges and opportunities associated with improving digital security for women. The findings underscore that women face unique digital security challenges, exacerbated by the increasing prevalence of cyberattacks. This highlights a critical need for enhanced protective measures tailored specifically to women's vulnerabilities. The analysis of gender-sensitive policies reveals a mixed perception of their effectiveness. While a significant number of respondents view these policies as beneficial, there remains a notable portion who feel they are insufficient. This indicates that while progress has been made in creating supportive policies, there is still a need for further development and refinement to better address the specific needs of women.

Furthermore, the strong endorsement of targeted educational programs suggests that such initiatives play a crucial role in improving women's participation in the cybersecurity sector. The positive response to these programs highlights their importance in bridging the gender gap and fostering a more inclusive and secure digital environment. Overall, the study emphasizes the need for continued efforts to enhance women's digital security through improved policies, targeted educational programs, and greater awareness of their specific challenges. Addressing these issues is vital for creating a safer and more equitable digital landscape. Future research should focus on evaluating the effectiveness of current strategies and exploring new approaches to better support and protect women in the digital realm.

To enhance digital security for women, it is crucial to develop and implement more robust and gender-sensitive cybersecurity policies. Organizations should focus on creating comprehensive strategies that address the specific threats women face, including targeted cyberattacks and online harassment. Additionally, increasing investment in educational programs aimed at women can help bridge the gender gap in the cybersecurity sector. These programs should be designed to offer practical skills and career guidance, encouraging more women to pursue careers in cybersecurity and thereby strengthening overall digital security.

Future research should investigate the effectiveness of specific gender-sensitive cybersecurity policies and their impact on women's digital security. Studies should also explore the long-term benefits of targeted educational programs in increasing women's participation in cybersecurity roles. Furthermore, research could examine the intersection of digital security challenges with other social factors, such as socioeconomic status and cultural background, to

develop more tailored and effective strategies for improving women's cybersecurity. Evaluating these areas will provide deeper insights into creating a more secure and inclusive digital environment for women.

Author declaration

Author contributions and responsibilities

The authors made major contributions to the conception and design of the study. The authors took responsibility for data analysis, interpretation and discussion of results. The authors read and approved the final manuscript.

Funding

This research did not receive external funding.

Availability of data and materials

All data is available from the author.

Competing interests

The authors declare no competing interests.

5. ACKNOWLEDGEMENT

We extend our sincere gratitude to all participants for their valuable insights and contributions to this study. Your willingness to share your experiences and perspectives has been instrumental in understanding the challenges and opportunities in improving digital security for women. Thank you for your time and commitment

6. REFERENCES

[1]. Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. IT professional, 12(1), 24-31. https://ieeexplore.ieee.org/abstract/document/5403174/

[2]. Berríos, N. (2019). Increasing the participation of young women in cybersecurity. Computer Science;. https://prcrepository.org/handle/20.500.12475/311

[3]. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. Human Behavior and Emerging Technologies, 2022(1), 2693080. https://uia.brage.unit.no/uia-xmlui/handle/11250/3080480

[4]. Dampier, D., Kelly, K., & Carr, K. (2012). Increasing participation of women in cyber security. In ASEE-SE Regional Conference, Starkville, MS. http://se.asee.org/proceedings/ASEE2012/Papers/FP2012dam133_520

[5]. Datta, P., Panda, S. N., & Bajaj, S. (2020, June). Data analysis of cyber security for women in haryana. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 763-767). IEEE. https://ieeexplore.ieee.org/abstract/document/9197788/

[6]. Egete DEle BAshishie D(2023)Unequal Culture of Women and Minorities in Cybersecurity DomainBritish Journal of Computer, Networking and Information Technology10.52589/BJCNIT-Q1MZPVWZ6:1(11-19)Online publication date: 5-Sep-2023. https://doi.org/10.52589/BJCNIT-Q1MZPVWZ

[7]. Fazil, A. W., Hakimi, M., Sajid, S., Quchi, M. M., & Khaliqyar, K. Q. (2023). Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province. American Journal of Education and Technology, 2(4), 50-61. https://doi.org/10.54536/ajet.v2i4.2248

[8]. Hakimi, M., Quchi, M. M., Hasas, A., & Fazil, A. W. (2024). The Transformative Power of Information and Communication Technology in Empowering Women in Afghanistan. Journal of Social Science Utilizing Technology, 2(1), 275-287. https://doi.org/10.70177/jssut.v2i1.702

[9]. Hakimi, M., Sazish, B., Rastagari, M. A., & Shahidzay, K. (2023). Artificial Intelligence for Social Media Safety and Security: A Systematic Literature Review. Studies in Media, Journalism and Communications, 1(1), 10-21. https://doi.org/10.32996/smjc.2023.1.1.2x

[10]. Hakimi, M., Shahidzay, A. K., Fazil, A. W., Khaliqyar, K. Q., & Quchi, M. M. (2023). Strengthening Resilience to Safeguard Women from Social Engineering Attacks in Afghanistan. Cognizance Journal of Multidisciplinary Studies (CJMS), 3(12), 88-97.

[11]. Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. International Journal of Gender, Science and Technology, 9(1), 25-44. https://genderandset.open.ac.uk/index.php/genderandset/article/view/449

[12]. Poster, W. R. (2018). Cybersecurity needs women. https://www.nature.com/articles/d41586-018-03327-w

[13]. Rowland, P., Podhradsky, A., & Plucker, S. (2018). Cybher: A method for empowering, motivating, educating and anchoring girls to a cybersecurity career path. http://hdl.handle.net/10125/50358

[14]. Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., ... & Hall, L. (2013, June). Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. In Proceedings of the ITiCSE working group reports conference on Innovation and technology in computer science education-working group reports (pp. 1-14). https://doi.org/10.1145/2543882.2543883

[15]. Toft, R. S. E., & Eikaas, T. C. (2023). The Impact of Gender Equality in the Cybersecurity Sector (Master's thesis, University of Agder). https://uia.brage.unit.no/uia-xmlui/handle/11250/3080480

[16]. Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's". Heliyon, 5(12). https://www.cell.com/heliyon/fulltext/S2405-8440(19)36514-4

[17]. Zahout, M. (2017). Women in Cybersecurity. McCloy Fellowship on Global Trends. https://www.acgusa.org/wp-

content/uploads/2017/08/McCloyFellowhip_Report-Zahout.

[18] Tamanna Quraishi, Nargis Hakimi, Musawer Hakimi, Maleena Safi, Fazila Akrami, Mursal Akrami, Khatera Akrami, & Zahra Nejrabi. (2024). Exploring the Enhancement of Educational Systems through Information and Communication Technology: An Investigative Study. *Journal of Social and Humanities*, 2(1), 21–30. https://doi.org/10.59535/jsh.v2i1.218

[19] Barge Gul Khalili, Tamanna Quraishi, & Sahar Fazil. (2024). The Influence of social media on Human and Social Communications: A Sociological Study. *Journal of Social and Humanities*, 2(1), 40–48. https://doi.org/10.59535/jsh.v2i1.246

[20] Risnandar, H., Maruapey, M. H., Iskandar, A. B., & Wahyudin, C. (2024). Effectiveness of Implementing the Government's Internal Control System in the District. *Socio-Economic and Humanistic Aspects for Township and Industry*, 2(4), 489–503. https://doi.org/10.59535/sehati.v2i4.339

[21] Tamanna Quraishi, Manila Hakimi, Samira Yashar, Qadria Jan Akhundzada, Shakiba Mosazada, & Somaya Azimi. (2024). The Role of Technologies on Women Entrepreneurship: A Case Study of Online University. *Socio-Economic and Humanistic Aspects for Township and Industry*, 2(1), 140–151. https://doi.org/10.59535/sehati.v2i1.237