Chapter-18

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

[1]Swati Pareek
[1]Student, IIHMR University

[2]Dr. Gautam Sadhu
[2]Professor, IIHMR University

DOI: https://doi.org/10.52458/978-8197040863.2024.eb.ch-18
Ch.Id:- IIHMR/NSP/EB/RHP/2024/Ch-18

INTRODUCTION

In the contemporary digital era, the significance of cybersecurity is escalating, given the growing exposure of businesses and individuals to diverse cyber threats. The positive impact of digital literacy on risk exposure is noted, while the interplay of online privacy concerns moderates the correlation between risk perception and exposure. Children exhibiting heightened privacy concerns experienced lower exposure, whereas those with enhanced digital literacy faced greater exposure. Safe online conduct necessitates a perception of risks as severe and a comprehension of privacy concerns. The intricate connection between online risks and benefits implies that factors influencing risk perception also influence perceived benefits. With the advent of cloud computing, the Internet of Things, and heightened technological reliance, cyber-attacks have evolved in sophistication and frequency.[1]

The research findings underscore that instructive parental mediation, which prioritizes communication between parents and adolescents, proves more effective in curbing information disclosure compared to restrictive mediation based on rules and control. Adolescents who shared their online experiences with parents displayed increased privacy concerns but did not necessarily adopt privacy protection behaviors. Positive associations were identified between online chatting and privacy concerns, while excessive Internet use, frequent engagement in social networking, and online gaming were linked to heightened information disclosure [2,3].

The study also revealed that privacy literacy training assisted children in recognizing low privacy risks, contributing significantly to our comprehension of how young individuals navigate online privacy. This has substantial implications for policymakers and educators. The investigation highlighted that teacher possessed moderate awareness across all concepts, while parents believed their children had moderate awareness, with the exception of cyberbullying, where high awareness was observed. Overall, the study underscores the importance of promoting responsible technology use among students, teachers, and parents [4].

RESEARCH QUESTION

1. Did the WNS Cybersmart project prove effective in reducing cybersecurity risks?
2. What were the students' perceptions of the Cybersmart project?
3. Could the WNS Cybersmart initiative be regarded as a successful cybersecurity endeavor?

RESEARCH OBJECTIVES

1. To evaluate the WNS Cybersmart project's implementation.
2. To assess the WNS Cybersmart project's success in lowering cybersecurity risks.
3. To determine how students' opinions on the Cybersmart project are perceived.
4. To develop a model to reduce cyber threats in kids.

RESEARCH METHODOLOGY

The research design adopted for this study was a mixed-method approach. The use of a mixed-method approach was deemed appropriate for this study as it allowed for a comprehensive analysis of the WNS Cybersmart project's effectiveness from both a quantitative and qualitative perspective. In this study, survey questions and interviews were used to gather data. The survey questionnaire was administered to school going kids. The questionnaire contained closed-ended questions that aimed to measure the effectiveness of the Cybersmart project in reducing cybersecurity risks and enhancing cybersecurity awareness among school going kids. Using Google forms for data collection. The data collected through the interviews were analysed using thematic analysis. The analysis of the data aimed to identify key themes and patterns in the data and to provide insights into the effectiveness of the Cybersmart project in reducing cybersecurity risks and enhancing cybersecurity awareness among school going kids. pie charts and bar graphs were used for pictorial representation of data.

RESULTS AND DISCUSSION

The analysis of the data reveals notable insights into the online behaviors, awareness, and perceptions of the surveyed group. In terms of age distribution, 58.3% of respondents were above the age of 10, while 41.7% were below 10 years old. A substantial 96.7% of respondents use the internet daily, emphasizing the significance of the online world in their lives. The devices used for internet access are predominantly mobile, with 73.3% utilizing mobile devices daily, while 23.3% use computers. The data indicate that over 50% of respondents spend more than 2 hours per day on the internet, highlighting a considerable online presence among children. Regarding cybersecurity awareness, Notably, more than 50% of respondents received cybersecurity training at school, showcasing the role of educational institutions in promoting online safety. The data reveals that over 78% of respondents are aware of common online threats, emphasizing the importance of educating children about potential risks. Additionally, over 80% of respondents understand the significance of keeping personal information private online. More than 86% of respondents are aware of the risks associated with online gaming and interacting with strangers. In terms of reporting cyberbullying incidents, Moreover,60% of parents have imposed rules and restrictions on internet usage, reflecting a proactive approach to ensuring their children's online safety. 80% of respondents are interested in learning more about cybersecurity and online safety at school, underscoring the demand for comprehensive education in this area.

CONCLUSION

The WNS Cybersmart project stands as a dedicated initiative with the core objective of advocating cyber wellness and responsible internet usage among students. This comprehensive project involves the implementation of diverse strategies and activities geared towards educating students on crucial topics, including internet safety, prevention of cyberbullying, online privacy, and the principles of digital citizenship. Central to its mission is the emphasis on cultivating a positive online environment and empowering students with the requisite knowledge, skills, and values to adeptly navigate the

complexities of the digital world. Importantly, the WNS Cybersmart project extends its impact by catering to the needs of students, parents, and teachers alike, envisioning the creation of a safer and more responsible online community for the young users of today.

REFERENCES

1. Teimouri, M., Benrazavi, S. R., Griffiths, M. D., & Hassan, M. S. (2018). A model of online protection to reduce children's online risk exposure: empirical evidence from Asia. Sexuality & Culture, 22, 1205-1229.
2. Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. Computers in Human Behavior, 54, 114-123.
3. Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in human behavior*, *110*, 106382.
4. Mıhçı Türker, P., & Kılıç Çakmak, E. (2019). An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents. Computers in the Schools, 36(4), 293-318.