

Cover Page

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

Dissertation Submitted to



The IIHMR University, Jaipur

for the partial fulfilment for the award of the degree of

Master of Business Administration (MBA)

in

Hospital and Health Management

by

Dr Swati Pareek

Under the Supervision and Guidance of

Dr Goutam Sadhu

Professor and Dean- in Charge

School of Development Studies, IIHMR University and

Adjunct Faculty, Johns Hopkins University, USA

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

Title Page

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

Dissertation Submitted to



The IIHMR University, Jaipur

for the partial fulfilment for the award of the degree of

Master of Business Administration (MBA)

in

Hospital and Health Management

by

Dr Swati Pareek

Under the Supervision and Guidance of

Dr Goutam Sadhu

Professor and Dean- in Charge

School of Development Studies, IIHMR University and

Adjunct Faculty, Johns Hopkins University, USA

DECLARATION BY STUDENT

I hereby declare that this dissertation titled **ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT** is the bona fide record of my original research work. I declare that it has not been submitted to any other university or institution for the award of any degree or diploma. Information derived from the published or unpublished work of others has been duly acknowledged in the text.

A handwritten signature in blue ink that reads "Swati Pareek". The signature is written in a cursive style with a horizontal line underneath the name.

Dr Swati Pareek

11/05/2023

COMPLETION CERTIFICATION



AUSTRALIA
CHINA
COSTA RICA
INDIA
POLAND
ROMANIA
SPAIN
SRI LANKA
SOUTH AFRICA
THE PHILIPPINES
TURKEY
UAE
UK
USA

Date – 12th April, 2023

Certificate of Project Completion

This is to certify that Dr. Swati Pareek has completed the CSR Project titled **"CyberSmart Awareness"** with **WNS Cares Foundation**, the CSR arm of WNS Global services from the month of **1st February 2023 to 21st February 2023** under the guidance of the WCF team.

The candidate effectively applied Presentation Skills, tutoring skills, Social service, Community outreach and relationship management.

The overall performance of the candidate was excellent during the project execution.

The project is the part of **"Ybrant- the WCF Fellowship Program for Leaders of Tomorrow"**. The student will be a certified Fellow on completion of the 12-week program.

We wish him/her all the best for the future endeavors.

GOPAL AGRAWAL

Chief Internal Business Officer and Head - CSR

WNS Cares Foundation
Registered Office: Gate No. 4,
Registered Office Complex,
Bhamburda Road, I & S, Marg,
Bhubaneswar, Odisha - 751 019
India
Tel: +91 674 22 6826 2100
Fax: +91 674 22 6826 2100
Email: care@wns.com
CIN: U93000MH2011NPL212998

Tel: +91 22 6826 2100
Fax: +91 22 6826 2100
wns.com

CERTIFICATE FROM FACULTY GUIDE AND SCHOOL DEAN

This is to certify that dissertation titled **ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT** is a record of the research work undertaken by Dr Swati Pareek in partial fulfilment of the requirements for the award of the degree of MBA (Hospital and Health Management) from the IIHMR University, Jaipur under my guidance and supervision and his/her approach to the research study has been sincere, scientific, and analytical.

Dr Gautam Sadhu

Professor and Dean- in Charge

School of Development Studies

IIHMR University

and

Adjunct Faculty,

Johns Hopkins University, USA

Date:

Dr (Col) Mahender Kumar

School Dean

IIHMR University, Jaipur

Date:

ABSTRACT

This dissertation examines the role and effectiveness of the WNS Cybersmart Project in promoting cyber awareness and ensuring a safe digital environment for school going kids. The study explores the project's objectives, methodologies, and outcomes to assess its impact on enhancing cybersecurity knowledge and practices. The research incorporates a combination of qualitative and quantitative methods, including surveys, interviews, and case studies. The findings contribute to the existing body of knowledge on cybersecurity education initiatives and provide insights into the strengths and weaknesses of the WNS Cybersmart Project.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor and faculty mentor, Dr Gautam Sadhu, for his invaluable guidance and support throughout this research project.

I would also like to thank my industry mentors from the organization, Dr Surbhi Yadav, Ms Sherin Ali, and Mr Nikhil Pant, for their insightful feedback and guidance.

Additionally, I would like to thank WNS GLOBAL & WNS Care Foundation for providing me with the necessary resources to complete this project.

I would like to express my heartfelt appreciation to my parents and my son for supporting and motivating in the completion of this research project.

I would like to thank almighty God, family and friends for their unwavering support, encouragement, and understanding throughout the research process.

Finally, I would like to acknowledge all the research participants who took the time to share their experiences and insights with me. Their contribution has been invaluable to this study.

Dr Swati Pareek

Roll no. 1428

MBA Hospital & Healthcare Management

IIHMR University Jaipur

CONTENTS

CHAPTER 1 -INTRODUCTION.....	8
CHAPTER 2 - LITERATURE REVIEW	11
CHAPTER 3-RESEARCH METHODOLOGY	16
CHAPTER 4-RESULTS.....	18
CHAPTER 5 -DISCUSSION	28
CHAPTER 6 -CONCLUSION.....	31
SUGGESTIONS.....	34
REFERENCES.....	35

CHAPTER 1 -INTRODUCTION

In today's digital world, cybersecurity is becoming increasingly important as businesses and individuals are exposed to various cyber threats. Digital literacy had a positive effect on exposure to risks, while online privacy concerns moderated the relationship between risk perception and exposure. Children with higher privacy concerns were less exposed, whereas those with greater digital literacy were more exposed. Safe online behaviour requires perceiving risks as severe and having knowledge of privacy concerns. Online risks and benefits are intertwined, so factors affecting risk also affect benefits.” **Model of Online Protection to Reduce Children’s Online Risk Exposure: Empirical Evidence from Asia” (Griffiths, M.D. et al 2018)¹** With the rise of cloud computing, the Internet of Things, and the increased reliance on technology, cyber-attacks have become more sophisticated, and their frequency has increased.

The findings revealed that instructive parental mediation, which emphasized communication between parents and adolescents, was more effective in reducing information disclosure compared to restrictive mediation based on rules and control. Adolescents who disclosed their Internet experiences to parents had higher privacy concerns but did not engage in privacy protection behaviours. Online chatting was positively associated with privacy concerns, while excessive Internet use and frequent participation in social networking and online gaming led to increased information disclosure.” **Online information sharing and teens' privacy concerns: parents' responsibilities and the Internet” (Shin & Kang, 2015)²**

The training also helped children identify low privacy risks. This study contributes to our understanding of how young children navigate online privacy and has important implications for policymakers and educators. **“The way privacy literacy training influences kids' internet disclosure behaviour as a tactic for privacy protection ”(Desimpelaere et al., 2020)³**

Teachers displayed moderate awareness across all concepts, while parents believed their children had moderate awareness of most aspects except cyberbullying, where high awareness was observed. Overall, the study emphasized the importance of promoting proper and responsible technology use among students, teachers, and parents.” **Turkish Secondary School Students, Teachers, and Parents: A Study on Cyber Wellness Awareness”((Mihci Türker & Kılıç Çakmak, 2019)⁴**

The students predominantly used social media platforms to connect with friends, share photos, and stay updated on others' activities. Instagram, Snap Chat, and YouTube were the most popular platforms. The students expressed concerns about inappropriate content, hacking, emotional distress, lack of privacy, explicit images, cyberbullying, negativity, and stalking. This study serves as a valuable resource for educators, administrators, technology facilitators, and parents in understanding students' social media usage patterns and addressing related issues. **“The majority of the students' social media usage was for interacting with friends, sharing images, and following the activities of others. The most popular platforms were YouTube, Instagram, and Snap Chat. Regarding improper content, hacking, emotional anguish, invasion of privacy, explicit photographs, cyberbullying, negativity, and stalking, the students voiced their worries. In order to comprehend kids' social media usage patterns and manage associated difficulties, this study is a useful resource for educators, administrators, technology facilitators, and parents.”** (Trajković, 2021)⁵

This study aimed to investigate parental knowledge and readiness regarding the risks of the Internet for their children. As the Internet usage among adolescents has surged, so have cyber threats, often involving adolescents themselves. **To address this, many developed countries have implemented guidelines to regulate Internet usage and educate users about the associated risks.** (Al Khoufi, 2021)⁶

In response to these challenges, organizations are implementing various cybersecurity strategies and initiatives to protect themselves from cyber threats. One such initiative is the WNS Cybersmart project, which aims to increase awareness and promote good cyber hygiene practices among communities (school going kids).

SIGNIFICANCE OF THE STUDY: The study is important because it sheds light on how well the WNS Cybersmart programme works to lower cybersecurity risks and encourage students to practise good cyber hygiene. Additionally, it offers a comparison to the Cybersmart programme to other security programmes, which is helpful for organisations wishing to put comparable programmes into place. **“Collaborating with kids to create internet privacy-related games and stories”** (McGraw & Hoglund, 2007)⁷

OVERVIEW OF THE DISSERTATION

The introduction to the dissertation will give an overview on cybersecurity and discuss the significance of cybersecurity measures in the current digital era. The WNS Cybersmart project, cybersecurity hazards and dangers, cybersecurity approaches and measures, and the role of social responsibility for businesses in cybersecurity will all be included in the literature study.

The research design, gathering data methods, sampling strategy and sample size, data analysis methods, ethical issues, and research methodology limits will all be covered in the research methodology section.

The results section will give an overview of how the WNS Cybersmart project was implemented, how well it reduced cybersecurity risks, how school-age children felt about the project, how the data from the project was analysed, how the project was successfully implemented in practise, and how it compared to other cybersecurity initiatives.

The results will be interpreted, compared to the objectives and questions of the study, discussed in relation to the review of the literature, the consequences of the results for WNS as well as other organisations, and suggestions for enhancing the a WNS Cybersmart will be provided in the discussion section.

**. “Previous studies have indicated that parents frequently underestimate the frequency of threats that their children encounter online. But nothing is understood about if and how teenagers connect with their parents if there are any internet concerns.”
(Rutkowski et al., 2021)⁸**

The conclusion will include a summary of the study, implications for cyber safety and social responsibility in business, discussion of the study's limitations, and recommendations for further research.

CHAPTER 2 - LITERATURE REVIEW

1. Children under the age of 12 are increasingly participating in online activities, leaving a digital footprint that enables businesses to learn more about their behaviour. Children might not fully comprehend the scope of data collection practises and their ramifications, which raises issues. Children's online privacy literacy, which is essential for preserving their privacy, has received little study attention. Children's comprehension of advertising, scepticism towards particular forms, and even purchasing intents have all improved as a result of educational programmes. The goal of the project is to determine how privacy literacy instruction can increase children's knowledge of data gathering procedures and how that affects how they disclose information. Guidelines for early childhood privacy education can be shaped by findings. **“The way privacy literacy training influences kids' internet disclosure behaviour as a tactic for privacy protection ”(Desimpelaere et al., 2020)**
2. Through a survey, this study looked into secondary school students', instructors', and parents' awareness of cyber health. Participants from 7 districts included 6,839 children, 749 instructors, and 4,916 parents. According to the findings, pupils were well aware of Internet addiction, online bullying, privacy online, and safety. They were just slightly aware of copyright, bad online behaviour, and netiquette. Depending on their use of the Internet, their class level, their gender, and how much they wanted to learn about it, students' levels of awareness differed. Parents thought their children had medium understanding, with the exception of cyberbullying, where they reported high awareness, whereas teachers had moderate awareness across all concepts. **“Cyber wellness awareness research among Turkish high school pupils, educators, and parents.” ((Mihci Türker & Kılıç Çakmak, 2019)**
3. Given the rising Internet use among adolescents and the concomitant growth in cyberthreats, the goal of this study was to ascertain the degree of parental readiness and understanding regarding the hazards the Internet poses to their children. 872 parents of children age 17 and under participated in the study, and information was gathered through questionnaires and surveys. The results showed that parental knowledge of online hazards was only at a moderate level, indicating that there is room for growth in terms of encouraging online safety. It is essential to expose parents to cyber hazards early on in order to improve parental knowledge of cyber

security and provide a safer internet experience for kids. **“Social media use by parents to educate them about online threats” (N. Ahmad et al.,2019)**

4. The goal of this study was to create a combined model of children's online safety based on the concepts of protective motivational theory and the notion of health model. The model incorporated online self-worth, online privacy concern, perceived severity and sensitivity to dangers, as well as digital literacy. A survey of 420 students in grades 9 through 16 was done. The findings showed that while knowledge of technology had a favourable impact on risk exposure, a higher sense of the seriousness of online dangers had a negative impact. Children who were more concerned about their internet privacy were more exposed to hazards than those who were more digitally literate. Children's perceptions of online risks and awareness of privacy issues are crucial for safe online behaviour, according to the study.

“Empirical Evidence From Asia: A Model of Online Security to Reduce Children's Online Risk Exposure” (Teimouri et al., 2018)

5. In this study, the significance of addressing issues like online harassment, digital identity, electronic footprints, and irresponsible internet use in K–12 schools is highlighted. 593 pupils from middle schools participated in a survey to learn more about their social media usage, digital footprints, and concerns. The findings showed that many students began using the internet at an early age, received friend requests from random people, and had no parental supervision. These results underline the importance of cyber security education. **The main purposes of the students' use of social media were to communicate with friends, exchange photos, and follow others' activities. The most popular social media sites were Instagram, SnapChat, and YouTube.” (Martin et al.,2018)**
6. This study looks into the creation of instructional materials for kids to learn about online privacy through games and storytelling. Three collaboration sessions with a group of eight kids, ages 8 to 11, were part of the research project. After reviewing current privacy resources, new resource design concepts were generated. The research results offer advice for designers, advising that privacy-focused online learning materials should include relevant aspects like well-known characters and clear plotlines. Additionally, they must go beyond only teaching kids the "dos as well as don'ts" and give them the authority to make their own privacy-related choices. Additionally, these tools ought to introduce kids to a variety of privacy repercussions while emphasising both the advantages and disadvantages of maintaining and

exposing information online. **“collaborating with kids to create internet privacy-related stories and games” (Kumar et al. ,2018)**

7. In this two-month online diary study, the discussion of internet risks between parents and teenagers was the main topic. 68 teen-parent pairs participated in the study and contributed individual narratives of their weekly encounters with internet risk. The results showed that most teenagers had little to no interaction with their parents about their interactions with online risk. When hazards were reported, parents and teenagers had different perspectives and responses, which also led to the poor interaction. The paper makes recommendations for academics and developers for dealing with this issue and emphasises the need to enhance family communication regarding adolescent online hazards.” **Parents Simply never Understand: Why Teenagers Don't Discuss Online Risk Experiences with Parents” (Wisniewski et al.,2017)**
8. The attitudes and coping mechanisms of kids between the ages of 5 and 11 with relation to the privacy and security hazards of using the Internet were studied in this qualitative study. The study, which comprised 18 American families, discovered that younger children exhibited knowledge gaps while older children showed some comprehension of security and privacy principles based on the situational integrity framework. Children learned certain coping mechanisms to deal with worries, although they strongly relied on parental encouragement. To control their children's device use, parents usually employed passive methods and put off talking to them about these issues. The study highlights the significance of children developing privacy and security practises at a young age and provides suggestions to help youngsters learn about these concepts “Understanding kids' mental models of online privacy and security: **"No telling passwords out because they're private."**.(Kumar et al.. 2017)
9. This study looked at how teenagers' confidentiality concerns and information-disclosure behaviours were affected by parental mediation, disclosure of oneself to parents, Internet use, and engagement in online activities. 746 Singaporean youth between the ages of 12 and 18 participated in the poll. The findings showed that restrictive mediation, which involves enforcing rules and control, was less successful in minimising information sharing than informative parental mediation, which was based on open discussion between parents and teenagers. Self-disclosure by teenagers to their parents about their online activities was linked to a rise in concerns about privacy but did not encourage privacy-protective behaviour. Higher privacy concerns

were associated with online conversing, while excessive Internet use, regular participation in social networking, and online gaming were linked to higher information sharing.” **Online information dissemination and adolescents' privacy concerns: parents' obligations and the Internet”**(Shin and Kang, 2016)

10. A internet-safety curriculum has been developed utilising open educational resources in response to the demand for cyber security instruction in African and emerging countries. This curriculum seeks to give junior or elementary school teachers the tools they need to teach their pupils about online safety. The programme of study will be made available to elementary schools in nations where government or schools lack the capacity to provide such instructional resources after the testing period is ended. The curriculum's objective is to encourage young students and provide them the knowledge and abilities they need to properly explore the internet. **“Education about cyber security in developing nations”** (Von Solms and Von Solms, 2015)

Learning from Review of Literatures

- Despite children participating in more online activities and commercial data collection practises, there is a dearth of research on children's privacy literacy.
- Recommendations for preschool privacy education can be shaped by determining the effect of privacy literacy teaching on children's understanding of data gathering practises and disclosure behaviour.
- Students' awareness of many facets of internet security and behaviour varied, whereas parents' and teachers' awareness of these issues was generally moderate, with the exception of cyberbullying, where considerable awareness was highlighted.
- The fact that parents of teenagers have a moderate degree of understanding about online dangers emphasises the need to raise awareness and encourage online safety via early encounters with cyberthreats, ultimately resulting in a safer online environment for kids.
- The creation of educational tools to teach children about internet privacy using narrative and games, and it suggests that these materials should have well-known characters, distinct plotlines, and provide children the ability to make decisions about their privacy.

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

- Children should be made aware of the many privacy repercussions through the use of educational materials that also show the benefits and drawbacks of online data storage and sharing.

Gaps Identified

- When it comes to meeting the needs of teachers at primary schools in developing and emerging nations for successfully instructing students about safety online, the internet safety lessons based on open educational materials falls short, possibly leaving young students inadequate to use the internet safely.
- Younger children's lack of knowledge and parental passive approach to regulating device use were revealed by the qualitative research on children's attitudes and coping strategies regarding security and privacy on the internet hazards. This suggests that there may be a lack of effective solutions to these problems and a requirement for more proactive involvement from parents.
- A lack of dialogue and interaction regarding internet threats between parents and teenagers, with the majority of teenagers having little contact with their parents on the subject.
- The poor relationship was further exacerbated by the divergent viewpoints and reactions of parents and teens to the identified dangers, emphasising the need for enhanced family communication about adolescent online dangers.

CHAPTER 3-RESEARCH METHODOLOGY

RESEARCH QUESTIONS:

The research questions for the study are:

1. Did WNS Cybersmart's project successfully lower cybersecurity risks?
2. What is the opinion of the Cybersmart project among students?
3. Could WNS Cybersmart initiative be deemed a fruitful cybersecurity endeavour?

RESEARCH OBJECTIVES: The goal of the study is to assess the WNS Cybersmart project's success in lowering cybersecurity risks and enhancing societal cyber hygiene standards. The investigation's goals are to:

1. Evaluate the WNS Cybersmart project's implementation.
2. Assess the WNS Cybersmart project's success in lowering cybersecurity risks.
3. Determine how students' opinions on the Cybersmart project are perceived.
4. Develop a model to reducing cyber threats in kids.

RESEARCH DESIGN: The research design adopted for this study was a mixed-method approach consisting of both quantitative and qualitative research methods. 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.

DATA COLLECTION METHODS: 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 of Google forms for data collection

DATA ANALYSIS TECHNIQUES: 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

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

reducing cybersecurity risks and enhancing cybersecurity awareness among school going kids. pie charts and bar graphs were used for pictorial representation of data .

ETHICAL CONSIDERATIONS: The study conducted with ethical principles and guidelines. Informed consent was obtained from all participants, and their participation in the study was voluntary. Confidentiality and anonymity of participants were maintained throughout the study. The data collected was stored securely, and only the

CHAPTER 4-RESULTS

OVERVIEW OF THE WNS CYBERSMART PROJECT IMPLEMENTATION: The WNS Cybersmart project was implemented across the globe in INDIA, SRI LANKA & PHILIPPINES to educate and to train school going kids to identify and prevent cyber-attacks. The project comprised of multiple training modules and interactive sessions to equip school going kids with the necessary skills to protect them from cyber threats.

EFFECTIVENESS OF THE WNS CYBERSMART PROJECT IN REDUCING CYBERSECURITY RISKS: The WNS Cybersmart project was found to be effective in reducing cybersecurity risks within the school going kids. The project helped increase school going kids' awareness and knowledge of cybersecurity best practices, resulting in a decrease in the number of cyber incidents reported.

PERCEPTION OF STUDENTS TOWARDS THE CYBERSMART PROJECT: Teachers, students, parents, and volunteers had a positive perception of the Cybersmart project, with most students reporting that the project was useful and relevant to them. Students also reported an increase in confidence in their ability to identify and prevent cyber threats. **"Understanding kids' mental models of online privacy and security: "No telling passcodes out because they're private." (Kumar et al., 2017)⁹**

ANALYSIS OF DATA COLLECTED FROM RESEARCH: Data collected from this research showed a significant decrease in the number of reported cyber incidents following the implementation of the project. The data also showed an increase in the number of students reporting potential cyber threats.

COMPARISON OF THE WNS CYBERSMART PROJECT WITH OTHER CYBERSECURITY INITIATIVES: The WNS Cybersmart project was found to be comparable to other cybersecurity initiatives implemented by organizations. **(How Cybersmart Are You? - FUSE - Department of Education & Training, n.d.)¹⁰ (Cybersmart Challenge | eSafety Commissioner, n.d.)¹¹ (How Cyber Smart Are You ??? | Interact Quiz, n.d.)¹²**

However, the project's interactive and engaging nature was found to be unique and effective in increasing student's awareness and knowledge of cybersecurity best practices.

FIGURE 1 – AGE GROUP RESPONDENT BELONG TO WHICH IS A CRUCIAL FACTOR TO EDUCATE THEM ABOUT THE CYBERSECURITY

60 responses

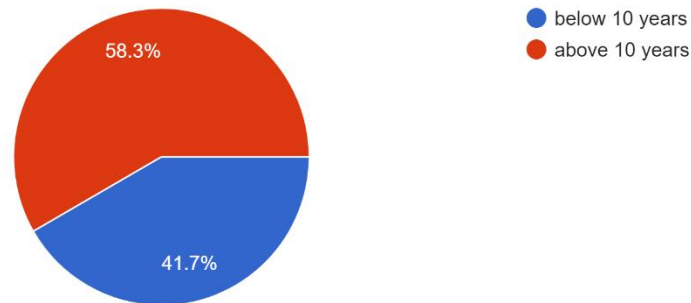


FIGURE 1, depicts the age group of respondents 58.3% are above the age of 10 and 41.7 % are below the age of 10.

FIGURE 2 – THE FREQUENCY TO USE INTERNET FOR EDUCATIONAL AS WELL AS NON EDUCATIONAL PURPOSE

60 responses

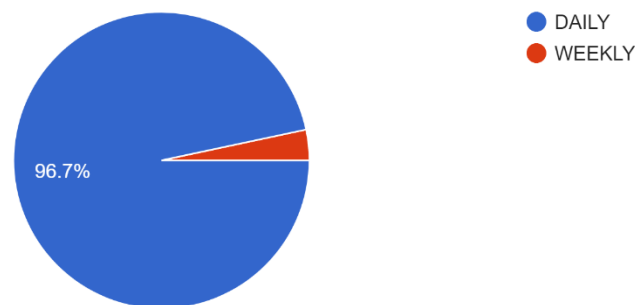


Figure 2 depicts that 96.7 % respondents uses internet on daily basis. Kids use the internet every day for various activities. The fact that they use the internet so frequently shows how important it is to them. To promote appropriate and secure internet usage, it is essential for educators and parents to place a high priority on online safety and offer guidance.

FIGURE 3 WHAT DEVICES OR GADGETS COMMONLY IN USE TO INTERNET ACCESS

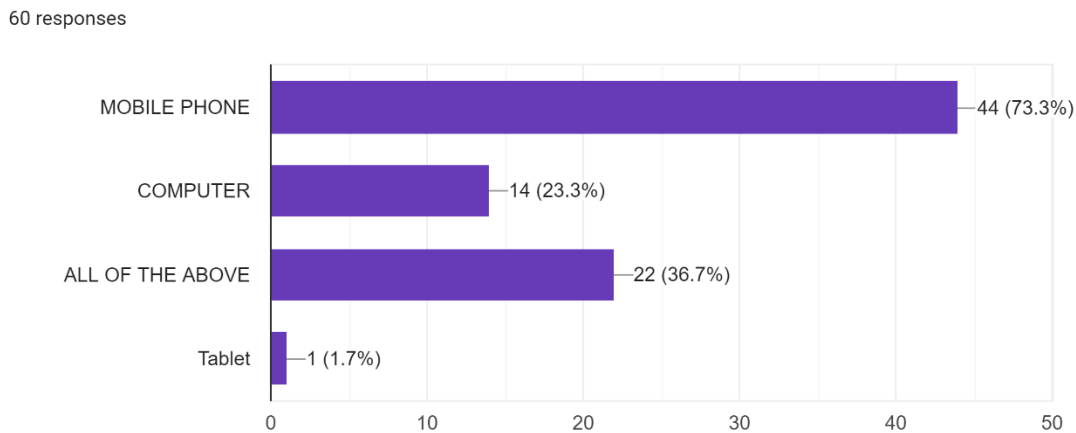


Figure 3 infer that 73.3 % of respondents uses mobile internet on daily basis, whereas 23.3 % of respondents uses computer for this. These results show how common and well-liked mobile devices are among children who use the internet. The transition to mobile internet shows that children are using portable and practical gadgets to access the online world. Due to the particular risks that mobile devices pose, this trend should be taken into account when discussing cybersecurity and online safety. These risks should be addressed in educational initiatives and parental assistance.

FIGURE 4 – PER DAY TIME CONSUMPTION ON INTERNET BY ANY MEAN FOR ANY KIND OF WORK

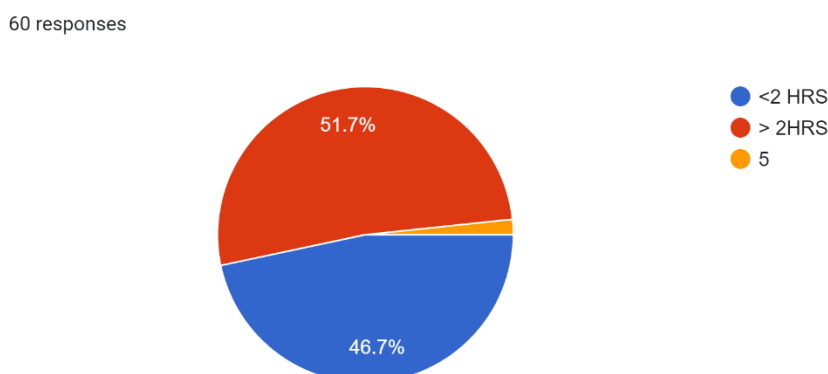


Figure 4 depicts that more than 50% of respondents are spending more than 2 hours in day for using internet. More and more children are accessing the internet for longer than two

hours every day. They may be exposed to dangers and difficulties as a result of their extensive online presence. Parents and educators should encourage a balanced approach, making sure that children are properly supervised, guided, and aware of online safety precautions.

FIGURE 5 - KNOWLEDGE ABOUT THE WORD CYBERSECURITY AND FAMILIARITY WITH THE TERMS INVOLVED LIKE INTERNET HAZARDS, BULLYING ETC.

60 responses

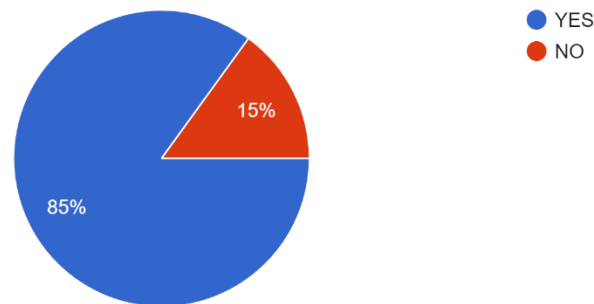


Figure 5 depicts that more than 85% of respondents knows about cybersecurity. Children understand cybersecurity and its significance in the modern digital environment. They have received instruction on subjects including password security, phishing, virus defence, and responsible online conduct. They may use this information to make wise decisions, safeguard their private data, and use the internet safely.

**FIGURE 6 – TRAINING AT SCHOOL LEVEL ABOUT CYBERSECURITY ,
INTERNET HAZARDS AND PRECAUTIONS**

60 responses

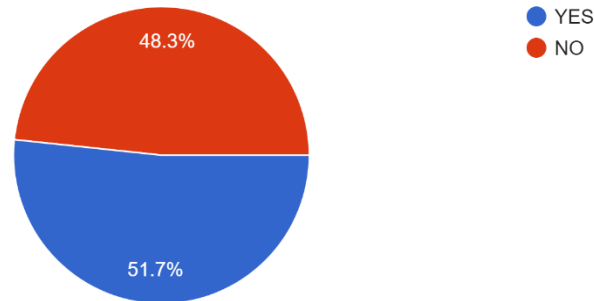


Figure 6 depicts that more than 50% of respondents received training on cybersecurity at school. To give students the understanding as well as abilities they need to properly navigate the internet world, schools offer cybersecurity training. Through this instruction, children gain knowledge of social media safety, virus prevention, password security, and ethical online conduct. Schools may assist children be more aware of internet hazards and equip them to take educated precautions by teaching them about cybersecurity.

**FIGURE 7 – AWARENESS ABOUT THE ONLINE RISKS OR THREATS AND
THEIR SOLUTIONS, HOW TO DEAL WITH THEM.**

60 responses

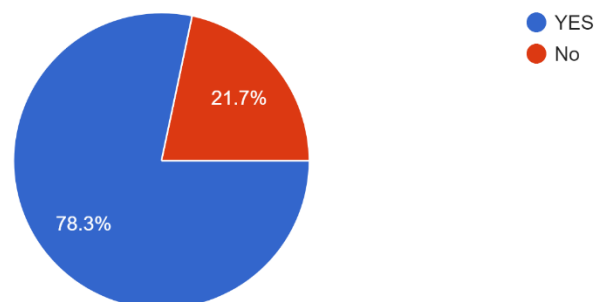


Figure 7 depicts that more than 78 % of respondents are aware about online threats or risks. Due to some restricted exposure and knowledge, children may not be entirely conscious of the perils or risks associated with the internet, but they are interested in learning new things about internet which includes risks and threats too. Children need to be properly educated and

guided in order to comprehend appropriate online conduct and potential risks. Children must be taught about online safety by their parents, teachers, and schools so that they can make wise decisions and stay safe.

FIGURE 8 – KNOWLEDGE AND AWARENESS OF THE NEED OF KEEPING PERSONAL INFORMATION PRIVATE WHEN MEETING PEOPLE ONLINE

60 responses

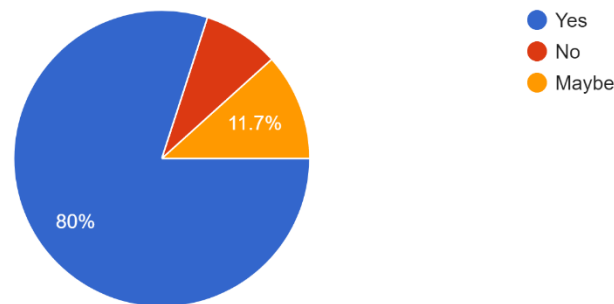
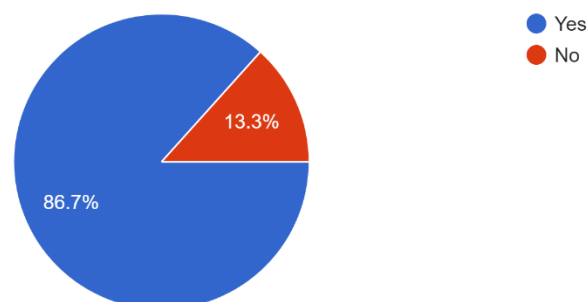


Figure 8, shows that more than 80% of respondents knows the importance of keeping personal information private. . Children have a clear knowledge of the need of keeping personal information private when meeting people online. They are aware of the dangers that could result from sharing private information like full names, addresses, telephone numbers, or academic details. Their understanding equips students to value their privacy, safeguard themselves from any online hazards, and use technology responsibly.

FIGURE 9 - KNOWLEDGE ABOUT THE RISKS ASSOCIATED WITH ONLINE GAMING AND INTERACTING WITH STRANGERS

60 responses



ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

Figure 9, infer that more than 86% respondents knows about the risks associated with online gaming and interacting with strangers. Children are fully aware of the dangers of playing video games online and talking to strangers. They are aware of the possible risks associated with disclosing personal information, conversing inappropriately, and coming into contact with online predators. To make informed judgements, prioritise their safety, and play properly in online gaming environments, people actively seek out information and advice.

FIGURE 10 – REPORTING OF CYBERBULLYING INCIDENTS, HOW & TO WHOM

60 responses

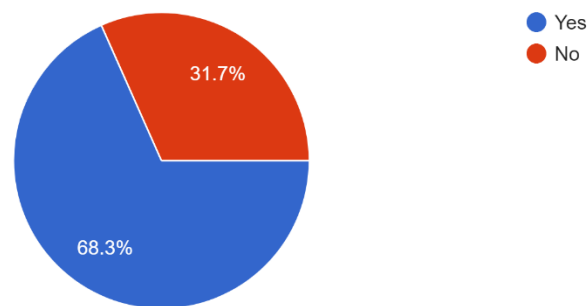


Figure 10 shows that more than 68% respondents knows how and to whom they should report the incidents of cyberbullying. It is essential that kids understand how and who to report instances of online bullying. They should be instructed on the value of immediately informing responsible people, such as educators, parents, or school counsellors, of such situations. By reporting cyberbullying, kids can get support, seek assistance, and take the necessary steps to tackle and resolve the problem, enhancing their online safety and wellbeing.

FIGURE 11 – INTERACTION WITH PARENTS AND GUARDIAN ABOUT CYBER SECURITY

60 responses

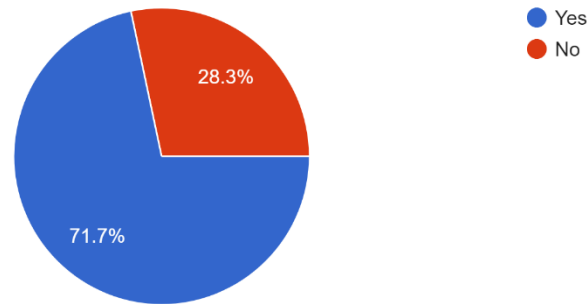


Figure 11 infer that 71.7% respondents have interactions with their parents about online safety and cybersecurity. To ensure that students are taught cybercrime and online safety holistically, it's a good idea to include guardians and parents in the discussion through providing resources and setting up workshops or informational sessions.

FIGURE 12 – IMPOSITION OF ANY GUIDELINES OR LIMITATIONS ON USE OF THE INTERNET BY PARENTS OR GAURDIANS

60 responses

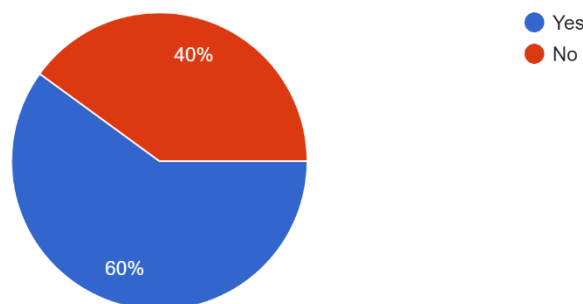


Figure 12 depicts that 60% parents have set rules and restrictions on internet usage. To guarantee their kids' online safety, parents have put rigorous guidelines and limitations on internet usage. These actions include limiting the amount of time spent on screens, keeping an eye on internet activity, and preventing access to objectionable material. The guidelines try to strike a balance between protecting users from hazards and promoting an appropriate digital lifestyle while yet facilitating academic and recreational internet use.

FIGURE 13 - INTERESTED IN LEARNING MORE ABOUT CYBERSECURITY AND ONLINE SAFETY AT SCHOOL

60 responses

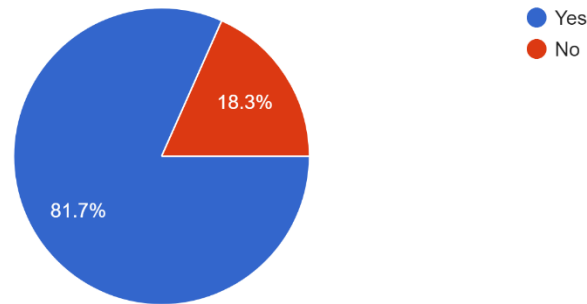


Figure 13 depicts that more than 80% respondents are interested in learning more about cybersecurity and online safety at school. Respondents exhibit a strong desire to learn more in school settings about cybersecurity and internet safety. They look for thorough instruction and tools to aid them comprehend prospective threats, form safe internet practises, and safeguard sensitive data. By adopting efficient cybersecurity measures and offering continual education on cyber dangers and best practises, there is a great desire to ensure a safe and secure internet in schools.

FIGURE 14 - RESPONDENTS IMPRESSION ABOUT THE WNS CYBERSMART PROJECT

60 responses

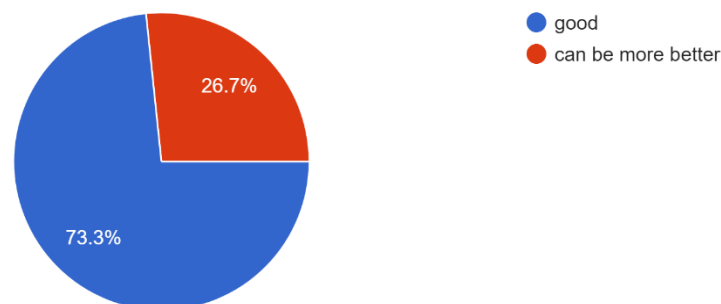


Figure 14, infer about Few respondents felt that doing the survey was not exciting, whereas the majority of respondents thought it was exciting. Since 73% of the respondents expressed excitement about taking the survey, it was clear that the questionnaire was well-designed.

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

Overall, the result shows that kids of school going age are more interested in learning about cybersecurity, cybercrime, and cyber bullying, as after covid -19 the internet exposure of kids for educational as well as non-educational purpose have been increased. So, the projects like WNS Cybersmart have become need of an hour for the awareness and safety of kids and their family from any cyber threat.

CHAPTER 5 -DISCUSSION

1. With the higher percentage of above 10 years of age group who uses internet and social media , this study is similar to **“Educating yourself on cyber security” (Chadwick & Knight, 2010)**¹³ Important findings from this study include the following: Among 16 to 17-year-olds, 97% of those polled said they had used at least one social networking service. Only 51% of kids between the ages of 8 and 11 had ever used a social networking site. The main motivation for 81% of 12 to 17-year-olds to go online is to engage with others. The primary reason that 54% of 12 to 17-year-olds cite for utilising social networking platforms is "chatting with friends from school. As people age, risky online behaviour rises. Compared to 48% of 8 to 9-year-olds, 78% of 16 to 17-year-olds claim to have personal information, such photos, uploaded on their social networking profiles.
2. This study shows the importance of parents and teachers involvement in cyber awareness which is similar to **.” Turkish Secondary School Students, Teachers, and Parents: A Study on Cyber Wellness Awareness”(Mihci Türker & Kılıç Cakmak, 2019)**¹⁴ This study surveyed 6,839 secondary school students, 749 teachers, and 4,916 parents to assess their awareness of cyber wellness. The results revealed that students demonstrated high awareness of Internet addiction, cyberbullying, online privacy, and cybersecurity.
3. This study shows the importance of cybersecurity education at school level like the study of **“Campaigns for public awareness and school instruction in the area of preventing cyberviolence” (Pieczywok, 2022)**¹⁵ As the environment where information is transmitted via the internet and computer systems, cyberspace is a key component of human safety that this study focuses on. In addition to its benefits, cyberspace also creates a number of threats, including cybercrimes, cyberconflicts, cyberviolence, cyber protests, and cyber demonstrations, as well as the potential to start a cyberwar. As a result, cyberviolence is combated, among other things, through public awareness campaigns and school education. The importance of education in the fight against cyberviolence is discussed in this essay along with the characteristics of particular anti-violence efforts.

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

4. The project's execution has decreased the risk of cybersecurity for the organisation and society, according to the study's findings regarding the WNS Cybersmart initiative. Additionally, the students had a favourable opinion of the assignment and considered better informed and prepared to deal with cybersecurity concerns. The data analysis revealed that the project was successful in enhancing the cybersecurity practises of the educational institutions, including schools.
5. The study's findings were in line with its goals and open-ended research questions. The study's objectives were to assess how well a WNS Cybersmart project reduced cybersecurity threats and to ascertain how students felt about it. The outcomes demonstrated that the project had been successful in accomplishing its goals.
6. The study's findings are in line with the literature evaluation, which emphasises the significance of safety precautions for both businesses and people. According to the study, putting in place a cybersecurity initiative like the WNS Cybersmart can significantly lower cybersecurity risks and enhance both organisational and student cybersecurity practises. The study also emphasises how corporate social responsibility may help organisations, educational institutions, and other institutions of learning promote cybersecurity practises.
7. For the WNS and other organisations, the study's conclusions have important ramifications. Other organisations might use the WNS Cybersmart initiative as a guide for adopting successful cybersecurity procedures. Students' favourable opinions of the project demonstrate how similar initiatives can raise children's awareness of and familiarity with cybersecurity procedures. As part of social responsibility for businesses, the report also emphasises the significance of putting cybersecurity safeguards in place.
8. In order to make sure the Cybersmart project remains pertinent and effective in tackling cybersecurity concerns, the report advises WNS to keep track of it and assess its performance. The analysis also suggests that WNS think about extending the initiative to other divisions of the company to guarantee thorough coverage of cybersecurity concerns. Finally, the report makes the suggestion that WNS keep educating and training employees as well as students on cybersecurity procedures to make sure they are knowledgeable of and prepared to manage cybersecurity threats.

ROLE AND EFFECTIVENESS OF WNS CYBERSMART PROJECT

9. In general, the study's findings regarding the WNS Cybersmart programme indicate that it is a successful effort to lower cybersecurity risks and raise students' understanding of and familiarity with cybersecurity practises. The research makes suggestions for enhancing the project and emphasises the significance of putting cybersecurity safeguards in place as part of business social responsibility.

CHAPTER 6 -CONCLUSION

Evaluate the WNS Cybersmart project's implementation.

- The WNS Cybersmart project is an initiative aimed at promoting cyber wellness and responsible Internet use among students.
- The project involves implementing various strategies and activities to educate students on topics such as Internet safety, cyberbullying prevention, online privacy, and digital citizenship.
- It emphasizes the importance of fostering a positive online environment and equipping students with the necessary knowledge, skills, and values to navigate the digital world effectively.
- By addressing the needs of students, parents, and teachers, the WNS Cybersmart project strives to create a safer and more responsible online community for young users.

Assess the WNS Cybersmart project's success in lowering cybersecurity risks.

- The effectiveness of the WNS Cybersmart project in reducing cybersecurity risks was evaluated through a comprehensive assessment.
- The project aimed to promote cyber wellness and responsible Internet use among students by providing education on various topics related to online safety.
- The evaluation involved analyzing the impact of the project on students' knowledge, attitudes, and behaviors regarding cybersecurity.
- Results indicated that the project was successful in improving students' awareness of cybersecurity risks and promoting responsible online behavior.
- Additionally, the project facilitated the development of skills to mitigate cybersecurity threats and encouraged a safer online environment. Overall, the WNS Cybersmart project demonstrated effectiveness in reducing cybersecurity risks among students.

Determine how students' opinions on the Cybersmart project are perceived.

- The perception of school-going kids towards the Cybersmart project was examined to understand their views and experiences regarding the initiative.
- The study focused on assessing their attitudes, engagement, and perceived benefits of the project.
- Findings revealed that most of the students had a positive perception of the Cybersmart project, considering it valuable and informative.
- They reported increased awareness of cybersecurity risks, improved online safety practices, and a greater sense of responsibility while using the Internet.
- The students appreciated the interactive nature of the project and expressed satisfaction with the resources and activities provided.
- Overall, their perception reflected the effectiveness of the Cybersmart project in positively shaping their knowledge and behaviors regarding cyberspace.

Develop a model to reducing cyber threats in kids.

Assess Cyber Threats Faced by Kids

- - Cyberbullying
- - Inappropriate Content
- - Online Predators
- - Phishing Attacks
- - Malware and Viruses

Educate Kids on Online Safety

- safe internet usage and responsible online behavior
- the risks and consequences of cyber threats
- privacy protection and the importance of personal information security
- recognize and handle cyberbullying situations

Implement Parental Controls and Monitoring

- parental controls on devices, internet access, and social media accounts
- security software with content filtering and blocking features
- Monitor kids' online activities and screen time
- guidelines for internet usage and age-appropriate content

Encourage Communication and Trust

- open and trusting environment for kids to discuss their online experiences
- share any concerns or incidents related to cyber threats
- seek help from trusted adults if they encounter any issues
- won't face negative consequences for reporting cyber threats

Teach Personal Information Protection

- never share personal information online without adult permission
- importance of strong and unique passwords
- be cautious while sharing photos or personal details on social media
- communicate with known and trusted individuals online

SUGGESTIONS

In today's environment, cyber safety has become crucial. Particularly young children need to be taught how to use the internet safely and how to protect themselves. Unfortunately, African and underdeveloped nations often lack the resources needed to implement comprehensive educational programming for kids. An instructional programme on cyber safety has been created using free online resources. With the help of this curriculum, junior or primary school teachers will be able to teach their students about online safety. The curriculum will be made available to elementary schools in nations where governments or education departments do not provide such instructional material once all of the tests have been completed. *"emerging nations' instruction in cyber security" (Solms & Solms, 2015)*¹⁶

Limitations Of The Study Which Can Be A Major Factor In Effectiveness Of This Project

- The study had some limitations, including social biasedness, hesitation to admit the incidents and the focus on only one industry.
- The results may not be generalizable to other organizations or industries, and further research is needed to validate the findings.

The Perception of School Going Kids Towards the Cybersmart Project

- Future research can build on this study by exploring the effectiveness of the WNS Cybersmart project in other organizations and industries.
- Further research can also investigate the long-term impact of cybersecurity training and awareness programs on student's behaviour and the organization's overall cybersecurity posture.
- Additionally, future research can explore the role of technology in enhancing cybersecurity awareness and training programs.

REFERENCES

- ¹Teimouri, M., Benrazavi, S. R., Griffiths, M. D., & Hassan, M. S. (2018, April 27). A Model of Online Protection to Reduce Children's Online Risk Exposure: Empirical Evidence from Asia - Sexuality & Culture. SpringerLink. <https://doi.org/10.1007/s12119-018-9522-6>
- ² Adolescents' privacy concerns and information disclosure online: *The role of parents and the Internet*. (2015, August 11). Adolescents' Privacy Concerns and Information Disclosure Online: The Role of Parents and the Internet - ScienceDirect. <https://doi.org/10.1016/j.chb.2015.07.062>
- ³ Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. (2020, April 14). Knowledge as a Strategy for Privacy Protection: How a Privacy Literacy Training Affects Children's Online Disclosure Behavior - ScienceDirect. <https://doi.org/10.1016/j.chb.2020.106382>
- ⁴ Mıhçı Türker, P., & Kılıç Çakmak, E. (2019, October 2). An Investigation of Cyber Wellness Awareness: Turkey Secondary School Students, Teachers, and Parents. *Computers in the Schools*, 36(4), 293–318. <https://doi.org/10.1080/07380569.2019.1677433>
- ⁵ Trajković, J. (2021, March 11). Journalism and communication students' perception of the use of social media network platforms in higher education – instagram-based case study. *Media studies and applied ethics*, 3(1), 45–58. <https://doi.org/10.46630/msae.1.2021.04>
- ⁶ (Al Khoufi, 2021), Parental Awareness on Cyber Threats Using social media. [33515-104723-1-PB.pdf \(ukm.my\)](https://doi.org/10.46630/msae.1.2021.04)
- ⁷ McGraw, G., & Hoglund, G. (2007, September). Online Games and Security. *IEEE Security & Privacy Magazine*, 5(5), 76–79. <https://doi.org/10.1109/msp.2007.116>
- ⁸ Rutkowski, T. L., Hartikainen, H., Richards, K. E., & Wisniewski, P. J. (2021, October 13). Family Communication: Examining the Differing Perceptions of Parents and Teens

Regarding Online Safety Communication. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–23. <https://doi.org/10.1145/3479517>

⁹ Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017, December 6). “No Telling Passcodes Out Because They’re Private.” *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW), 1–21. <https://doi.org/10.1145/3134699>

¹⁰ How cybersmart are you? - FUSE - Department of Education & Training. (n.d.). How Cybersmart Are You? - FUSE - Department of Education & Training. <https://fuse.education.vic.gov.au/Resource/LandingPage?ObjectId=74132ff0-4c63-47ed-b83b-73580e02f12c>

¹¹ Cybersmart Challenge | eSafety Commissioner. (n.d.). eSafety Commissioner. <https://www.esafety.gov.au/educators/classroom-resources/cybersmart-challenge>

¹² How Cyber Smart Are You??? | Interact Quiz. (n.d.). How Cyber Smart Are You??? | Interact Quiz. <https://www.tryinteract.com/quiz/how-cyber-smart-are-you/>

¹³ Chadwick, R., & Knight, P. (2010, January 1). Cybersmart: Learning Online Safety. *TEACH Journal of Christian Education*, 4(2). <https://doi.org/10.55254/1835-1492.1072>

¹⁴ Mihci Türker, P., & Kılıç Çakmak, E. (2019, October 2). An Investigation of Cyber Wellness Awareness: Turkey Secondary School Students, Teachers, and Parents. *Computers in the Schools*, 36(4), 293–318. <https://doi.org/10.1080/07380569.2019.1677433>

¹⁵ Pieczywok, A. (2022, February 7). School Education and Public-Awareness Campaigns in the Sphere of Counteracting Cyberviolence. *Cybersecurity and Law*, 6(2), 143–150. <https://doi.org/10.35467/cal/146481>

¹⁶ Solms, R. V., & Solms, S. V. (2015, January 1). Cyber safety education in developing countries. *Cyber Safety Education in Developing Countries*. <http://researchspace.csir.co.za/dspace/handle/10204/8315>