# Investigating levels of cybersecurity risk awareness by South African Parents

**Hangwelani Masutha**

**1884336**

**1884336@students.wits.ac.za 0829304730**

**A research proposal submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business**

**Johannesburg, 2022**

## ABSTRACT

The rapid development in technology and easy accessibility to the internet has resulted to an increase in cybersecurity challenges on a daily basis. Children get introduced to the internet at an early age when they still have very low levels of perception. As a result, children get exposed to cybersecurity risks such as cyberbullying, cyberstalking, stranger danger, identity theft and phishing scams. These necessitates parents' awareness of such risks as parents play a vital role in ensuring safety and teaching safe practices in order to protect children while they navigate the internet.

This research examined the levels of South African parents' cybersecurity risks awareness and knowledge which children face when interacting on the Internet. It also examined the role parents play in educating their children on such risks and examined whether parents applied appropriate security measures in order to protect their children while accessing the internet.

The research used quantitative methods to collect data. A survey of parents with children between the ages of 3 and 12 years who live with their children in the households, was undertaken.

The results showed that that although majority of the parents were aware and knowledgeable of the cybersecurity risks, lower levels were evident on parents educating their children of those risks and lower levels were also reported on the application of security measures. Therefore, children were still compromised and exposed to such risks while they access the internet which necessitates parents further improving on educating children and also applying necessary security measures in order to protect them while accessing the internet.



## KEYWORDS

cybersecurity risks, cybersecurity awareness, internet, children, parents awareness, cyberbullying, cyberstalking, phishing, stranger danger, identity theft

## DECLARATION

I, Hangwelani Masutha, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Hangwelani Masutha Signature: 

Signed at …Venda……

On the 29…….. day of ……June…… 2023…..

## DEDICATION

This paper is dedicated to my beloved family, my husband and our 3 kids. Your support and words of encouragement has given me the drive and sustained me in getting this to completion.

To my mother who is passed on, you have taught me that trusting God in everything I do, putting in the work and determination always pays off. You were an embodiment of what grace, patience and loving what you do looks like and that has kept me going through this journey.

## ACKNOWLEDGEMENTS

Special thanks to my supervisor for your guidance and patience. I know without your help; this would not have been possible.

My pastor (Pastor VTJ Masakona) for praying for me and using his church as part of the participants. I am really humbled and will forever be grateful.

To my colleague Manqoba Mngomezulu, thank you for sharing making yourself available and sharing your own knowledge and your book as a Security officer.

And finally, my nanny who takes care of my kids and my newborn baby. It hasn't been easy working on the paper with a newborn in the house but, you have made it easy for me focus on the paper and held the fort with ease and grace.

# TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# CHAPTER 1. INTRODUCTION

## 1.1 Statement of purpose

The purpose of this quantitative research is to examine the levels of awareness and knowledge of South African parents with respect to the cybersecurity risks which are introduced through their children accessing the internet. It investigates the extent to which parents are engaging and educating their children on the various available online safety practices. It also examines if parents have the necessary tools in place to protect their children while on the internet.

According to “The Bill of Rights of the Constitution of the Republic of South Africa” (1996), a child is defined as a person under the age of 18 years. The Constitutional Court emphasises the importance of the protection of children as they are the most vulnerable members of society who are still dependent on parents or families to care and protect them. In a study conducted by Wayman (2017) of eleven African countries, South Africa had 23% of children aged between 9 to 11 performing three or more social activities online on a weekly basis. The study also highlighted that there are children as young as an average age of 4.9 years who are already starting to access the internet.

Kesavelu, Sheela, and Abraham (2021) highlighted the different stages of child development. They noted stage 3 as pre-school age of between 3 and 5 years, where they start developing interaction with peers and neighbours. Stage 4, which is approximately 6 to 12 years, is said to be an early school age of a more social interaction. Both these stages are children, who are still developing and therefore still vulnerable (1996).

The focus of this study is on parents or care givers living with children in their households between the ages of 3 and 12 years. According to a paper on Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace (2021), children do not have the ability to comprehend social risk concepts which can comprise their safety while they are online thus parents’ protection and guidance on safe ways of using the internet are critical,

## 1.2 Background of the study

**Internet adoption**

South Africa has seen an increase in the rollout and adoption of broadband fibre technology which enables faster and better internet connectivity. Network service providers like Telkom have increased fibre rollout from 38% in 2019 to 51% in 2021 which equates to approximately 280 000 homes. In addition, they have also increased their mobile customer base to 15,3 million with an increase of 27.8% from 2019 to 2021.The total number of mobile users in South Africa that connected to the internet in 2021 amounted to 34,45 million which is more than half of the total population (Statista, 2021).

The increase and improvement in the accessibility of the internet, has created a dependency and has made the internet an integral part of society. Services such as the delivery of education are now not only limited to the traditional brick and mortar delivery methods but can now be delivered beyond geographical locations through online school platforms. The results of this technological advancements have also led to an increase in the diversity of users including children. As shared in the UNICEF report (2019), children not only use the internet for education purposes but also for social online activities such gaming, sharing of music, videos and ideas. The report further reported that globally, one in every three children is an internet user and is under the age of 18 years.

**Risks Introduced**

Despite its various positive contributions to society, the internet also introduces many associated cybersecurity related risks. Amongst others are, cyberbullying, access to inappropriate sites content such as pornography, and online friendships developed with unreliable people like paedophiles (Ahmad et al., 2019). These are risks which often target children specifically due to their low levels of perception AlShabibi and Al-Suqri (2021).

**Need for awareness.**

While there is a need for children to be aware of cybersecurity risks, it can be challenging for young children to fully comprehend the risks inherent in accessing the Internet. It is important that parents and care givers are involved to help protect children and prepare them for future when they become unmonitored independent users of the internet (Pietre-Cambacédes, 2010, as cited inRenaud & Prior, 2021).

A research study by the United Kingdom's (UK) government regulator (Ofcom, 2020) highlighted that 8 in 10 parents are concerned about their children being exposed to harmful internet content. Their top five concerns were on cyberbullying, sexual or pornographic content, violent content, people pretending to be someone else and their children spending too much time on the internet.

The survey conducted by UNICEF South Africa (2022) showed that 25% of children have added people that they do not know and have never met on their online contact list, 18% have shared photos with strangers and 67% have sexual image content shared with them on their online accounts. The study also reported that there are incidents where children have been sexually exploited while online and they preferred not to share those traumatic experiences with the adults to obtain help. This in turn has a long-term impact on the children from a mental health and wellbeing perspective in their adulthood stage.

Research further shows that parents do not always have the necessary skills to enable them to effectively mediate and help their children stay safe online (Livingstone et al., 2017).

Several studies as far back as 15 years ago have already explored the cybersecurity risks which children are being exposed to while connected to the internet. (Singh, 2008) focused on the parents and investigated if they have some level of awareness with regards to the dangers that come with being online and how they are responding to them to protect their children. The dangers which the researcher focused on were pornography, paedophilia, adverts for products and drugs, propaganda, violence, and chat rooms. The findings from the research highlighted that, some of the parents were aware of these dangers and they had put some measures in place to protect their children, which include supervision

of online activities and implementing software internet security control to filter pornographic content.

In a 2015 study (Butler & Butler) looked at whether the online South African consumers are managing their computer passwords, to determine whether they are in line with their perceptions around their capability for secured password management measures. The research found that there were some disparities.

A study by Toit, Hadebe, and Mphatheni (2018) looked at the South Africans' public perception of cybersecurity and the different experiences by south Africans on cybercrimes. They identified that some respondents do have some understanding of the concepts and have experienced some of the related attacks, like online harassment, cyberbullying, identity theft via email or SMS and malware attacks.

## 1.3 Research problem

The increase in the use of the internet has resulted to the expansion and diversification of the user community, which includes children. With this increase in the number of users, cybersecurity risks have also increased. Some of the risks which children face include child cyber trafficking, exposure to pornography, cyberbullying, online harassment, phishing, cyberstalking, stranger danger and identity theft. UNICEF (United Nations Children's fund) research paper noted that the impact of these risks if successfully perpetrated on children can become detrimental as that can have psychological and physical harm to the child, where cases such as suicide becomes the end results(2019)

Due to the continuous increase in the use of the internet, the awareness of cybersecurity risks by parents is still a concern in ensuring their children safety. Parents limitation on skills or knowledge to mediate their children's safety, the need for bringing to light the recommendations on safety measures which parents may apply to keep children safe online remain a gap as also highlighted in recent studies. Cilliers and Chinyamurindi (2020) highlighted the inability of parents' to educate children on safe ways of using technology and not knowing how their children interact on the internet while Chipangura and Dtendjo-Ndjindja (2022)

highlighted that some parents never discuss cybersecurity risks with their children. This study research investigates the levels of awareness of such risks, determines whether parents actually educate their children of the risks and if they also apply the necessary security and monitoring measures.

## 1.4 Research questions

In order to investigate, the following research questions were posed in response to the research problem:

1. To what extent are parents knowledgeable of the cybersecurity risks which can impact their children while accessing the internet?
2. To what extent are parents educating their children on the safety practices while connected to the internet?
3. To what extent are parents implementing proactive security and monitoring measures to protect and monitor their children's online activities?

## 1.5 Rationale

Cybersecurity risks towards children have become a constant topic across the globe. This is due to the children's vulnerability and inability to not always being able to protect themselves while using the internet. Thus, continuous awareness by parents of these security risks is critical to reduce or prevent impacts on children. The parents' awareness is therefore the underlying concept of this research to be able to determine if parents are keeping themselves up to date on the evolving cybersecurity risk and are respectively applying the knowledge, they are gathering with regards to the preventative security measures

A recent South African survey conducted by UNICEF in 2022 highlighted the continued exposure of South African children to cybersecurity risks with the study noting 67% of children having reported to have seen sexual images on an online device. 70% were reported to use the internet without parental consent, while 25% have added people whom they have never met as friends in their contact list and 18% having sent photos or videos of themselves to a person they

have never met. The same survey highlighted only 41% of children having received “some” information on online safety.

Due to the survey being quite recent, this research will play an important role in assessing whether parents are actually aware of the cybersecurity risks (*and to what extent*) and further socialise the risks to the parents and encourage them to get more involved in protecting their children while they are using the internet.

## 1.6 Delimitations of the study

Lange (2012) highlighted that, the role players that need to be involved in socializing and encouraging good internet practices are the schools, teachers, learners, parents, and guardians. This research study will primarily focus on the cybersecurity awareness of South African parents or guardians with children between the age of 3 and 12. The research will focus on parents who are able to actively monitor their children internet activities not focus on who do not physically live with their children.

## 1.7 Definition of terms

Cybersecurity. “The ability to protect or defend the use of cyberspace from cyber-attacks” (NIST, 2012)

Cybersecurity awareness. “Level of appreciation, understanding or knowledge of cybersecurity or information security aspects. Such aspects include cognizance of cyber risks and threats, but also appropriate protection measures”(Nurse, 2021)

Cyberbullying, “ Involves sending or posting harmful or cruel text or images using the internet (e.g., instant messaging, e-mails, chat rooms, and social networking sites) or other digital communication devices, such as cell phones”(Feinberg & Robey, 2009)

Cyber safety. “Consists of actions individuals take to minimize the dangers they could encounter when using the internet-capable technology. Cyber safety issues

include online predators and unwanted communications, viruses, and spyware”(Pusey & Sadera, 2011)

## 1.8 Assumptions

This study assumes that the participant’s answers are honest. There may be perceptions which parents hold based on what they believe are social standards. They may feel that there is a certain awareness expectation which they need to have and therefore not answer questions based on the true reflective sense but based on how generally they answer should be. The structure of the questions for this research’s survey have included multiple choices in order to allow the participants ability to assess and answer the questions from an individual reflective sense in order to address this assumption.

The study assumes that parents are literate and can read and write therefore, they can complete the questions. It also assumed that the participants will be people living with children in their household are able to supervise them.

## 1.9 Chapter Outline

The following chapters of this study present the literature on the related topic on parents’ awareness, and the research methodology which was used to evaluate the current state of the awareness in South Africa, which elaborated the data collection procedure followed. Following that, chapters on the presentation of the data analysis results, discussion of the results and a chapter with conclusion and recommendations were presented.

# CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

## 2.1 Introduction

The following literature discusses and critiques previous works research on the levels of parents' awareness of cybersecurity risks exposed that children are exposed to. It starts with reviewing the literature that assesses parents' knowledgeability of the cybersecurity risks which impact children. Following that, it touches on research done around the extent of the involvement or engagements by parents in educating their children about the cybersecurity risk and lastly look at whether parents are applying different proactive measures or monitoring tools on the children's devices to try and minimize the risk exposures.

## 2.2 Definition of topic or background discussion

As highlighted in previous sections, the involvement of parents in instilling safety practices in children while accessing the internet remains critical. This study sought to determine the level of cybersecurity risks awareness by South African parents with the intent to identify areas of improvement to extend their knowledge and also add to the body on knowledge around parents' awareness in South Africa.

## 2.3 Parents Knowledgeability of cybersecurity risks which impact children.

Several research studies across the globe have put focus in creating awareness to cybersecurity risks and showed the importance of putting more focus on children who are the most vulnerable. Due to the children's low level of understanding, AlShabibi and Al-Suqri (2021) have noted that besides teachers at schools, families including parents play an important role in improving children awareness. Furthermore, parents reported concerns of lacking knowledge due to the constant evolution of cybersecurity landscape and continued increase in the

number of children accessing the internet at an early age. It is necessary for parents to continuously revisit their awareness and knowledge of these changes in the cybersecurity space in order to help parents retrospectively recognize where they have gaps and need to improve themselves to keep their children safe while online.

### *2.3.1 Lack of Knowledge*

In the South African context, previous research conducted by Mariska (Lange, 2012) found that at times, parents do not have any online safety practices emphasized in the households, thus allowing their children to freely access the internet for long hours, privately in their rooms, without any need of preapproval or even any supervision. The researcher further highlighted that the cause of most risks is as a result of human behaviour. This therefore concluded that some of the parents are not necessarily taking accountability or responsibility of their children's online safety and therefore not prepared to instil online safety awareness on their children.

As highlighted in the internet adoption section of the previous background section, internet use is now beyond just educational purposes for children but also for social and gaming purposes. Therefore, as children are engaging in the internet, personal and sensitive data is being captured, stored, communicate and processed (Lange, 2012). Thus, it is of utmost importance that as users of the internet, together with their parents are informed, aware to protect themselves from unintentionally sharing the sensitive information.

Willard (2007) had previously shared the different risks which young people are exposed to while on the internet which remain relevant in the current day. Some of those risks include exposure to inappropriate sexual content like pornography, cyberbullying, identity theft scams, online gambling etc. Bioglio et al. (2018) had shared a social network simulation game to raise privacy awareness among children. On the study by Prior and Renaud (2020), they shared some guidelines on the password best practices which parents and educators can use to prepare children for good password practices which include good password creation

practices like making your password hard for other guess and password retention to make sure it gets changed after a period of time.

Kortjan and Von Solms (2014) also highlighted in their study the lack of cybersecurity awareness, due to little government and education initiative sponsorships and thus proposed a framework to help South Africans become aware of the cybersecurity risks. The target of the framework included parents and guardians, as they are the one who's role is to primarily protect the children who are vulnerable.

Kritzinger (2017) noted on her research around growing cyber safe culture for school learners, the lack of parents' knowledge and confidence in addressing cyber risks which in turn can result to cases of cyberbullying which is also reported as major concern by Mariska Lange. Kritzinger (2014) also looked at the different cyber risks which her school learners survey participants have been exposed to. Some of the ones which were most significant were on cyber-bullying, pornography sites and identify theft, stalking, virus and malware. Such findings highlight the need for parents to also continuously be involved in the fight for protection of children against such perpetrators, by continuously revisiting their knowledge and awareness of these cyber risks.

A research article titled "**Stranger Danger! Social Media App Features Co-designed with Children to Keep Them Safe Online"**(2019) have noted incidents related to mobile applications such as TikTok where children were engaging with strangers through the mobile applications. Part of the research questions was to assess how children think about and understand stranger danger in online context. The findings highlighted that the understanding of the concept was mainly on the offline context rather than online context.

Phishing attacks are some of the biggest security risks target users accessing the internet or digital space which consists of attempts to steal sensitive information (like credit details, user's identity etc.) using fake email, fake website and social media messages. Alwanain (2021). Furthermore, the experimental research by Alwanain (2021), revealed that training on phishing awareness has significant

positive effects on the ability of children using WhatsApp to identity phishing messages which in turn avoids attacks.

Globally, similar findings have also been reported where parents' knowledge of internet risks exposed to children is shown to be lacking. Ljubojev, Glusac, and Radosav (2017) investigated the parents' perceptions and protection of their children on the internet in the republic of Serbia. A question on whether parents were aware of any inconveniences their children have experienced was asked. A few options were provided and among others included exposure to sexual content, aggressive content, abuse of the child, unplanned misuse of cash expense etc. From the options provided a huge number of the parents respondents reported that they did not know if their children had experienced any of the cases highlighted in the options, with some only choosing one or two from the list provided. Therefore, the findings reported a low level of awareness as parents have shown lack of knowledge of their children internet experiences.

Lester (2018) investigated the cyber safety awareness among parents and teachers from ways of monitoring internet use, knowledgeability of the safety issues and how they learn and stay up to date on cyber safety topics. What came out from the findings of the surveys and interviews conducted was that parents monitor their children's online activities through supervision when children are accessing the internet in the same room, they checked the browser history and also the make use of software to track the visited sites. However, they also highlighted that although they are monitoring, there are still cases where children are able to navigate around the monitors in place and find themselves in trouble through by-passing the filters applied by the monitoring software. This highlighted that children are always a step ahead of the parents on technology as these are children born in the technology age. This emphasizes the need for parents to always keep themselves up to date on these changes to learn better ways of protecting their children. The findings also highlighted the need for continuous learning by parents due to continuous rapid changes in the technology space as they were not aware of some technology aspects like ghost application which they highlighted to not being aware of such. These are applications that have

ability to be hidden behind images which children are now using to hide application which they know their parents would not approve.

On the other hand, there are countries where parents are reported to be managing the awareness of these risks well to ensure their children are protected while on the internet. UK is one of the countries which are ranked high on mediating for their children' safety. Parents monitor the websites visited by their children and they are able to also apply filters and block unwanted website content. They discuss with their children why certain website are good and which ones are bad, therefore educating their children on the safety practices.(Annansingh & Veli, 2016)

### *2.3.2 Cyber risks and its impact on children*

The introduction of technology has brought about a lot of benefits, from convenience of online schooling, children being able to communicate with their peers without being physically in the same place, more access to information etc. However, the same technology can have some negative impacts, particularly on children who are most vulnerable and can affect their social development.

According to UNICEF (2019) programme report on adolescent development, children of the ages between 10 and 19 start to develop new ways of interacting with the world including how they engage with people outside their family circles. This stage is where children strive to standout or have a sense of belonging in the society and within circles of friendships which they develop. It is at this stage where; the negative effects of the social media can affect children since they are still vulnerable to things like peer pressure. KOCOGLU (2021) has highlighted the alienation which an individual can develop due to social media. The individuals seek validation from their social networks which they develop and create a new self-image based on groups of individuals' expectations, instead of striving to identify who they are as individuals. Kocoglu (2021) noted academic studies have emphasized the negative impact on the sense of belonging, which the search of identity in the digitalized world has on an individual. Bacıoğlu (2022) on the research around cyber risks awaiting children, supported this notion and noted that the long hours spent on social media by children and teenagers may result

to negative emotions such jealousy, depression, and low self-esteem, also due to the lack of validation which is sometimes not received after one presents themselves to their followers. (*For example, not getting expected "likes" on pictures or videos which individuals would post of themselves).*

Bacıoğlu (2022) also supports the notion that cyberbullying is one of the major risks impacting children and adolescents, also highlighting factors from previous research such as exposure to violence, family upbringing and moral assignments as some of the side effects contributing to the behaviour.

Such behaviours can be picked up through supervision by parents if they are involved in monitoring the content shared and received on the internet by children and immediately address and correct the behaviour at the early stages of their children' s lives.

More risks were reported also with cyberbullying as the highest risk statistic by Kritzinger (2017). She conducted a survey on the South African primary school learners, who reported on exposure to pornographic sites, thieves getting access to their residential addresses and identity theft as some of the potential risks with very high scores. Following to this, a significant number of leaners also reported that they have access to the cell phones without a need for permission from their parent. A notable percentage of parents also reported to not monitoring their children's internet activates. These are concerning statistics and require parents to be made aware of the risks exposed to children when they are not involved in their internet supervision.

### *2.3.3 Hypothesis 1*

The level of knowledge of cybersecurity by parents influences the level of cybersecurity risks exposure on children while they are on the internet.

## 2.4 Parents educating their children on the safety practices while connected to the internet.

### *2.4.1 Education of children by Parents*

On the research by Marais (2012), he noted that “children are the adults of tomorrow”, therefore it is the parents responsibility to ensure their children develop into responsible adults of tomorrow. He further highlighted the importance of education as one of the important controls which parents should consider, noting that the days of physical supervision of internet activities when computers would be situated in the living room and chilren use the computer in same room with them have long passed. Chilren are now using mobile phones and are able to access the internet in their private spaces or their rooms. This intruduces a great risks as some children are able to bypass the restrictions applied on the devices by the software filters. This emphasizes the need to educate children on safe ways of using the internet. Marais’s research findings highlighted the lack of education to children by parents, attributing to further exposing children to the risks that come with them accessing the internet uninformed. This led to him introducing a framework which requires parents to first self educate through gaining knowledge on mobile usage risks and interventions methods, then educate the child by creating awareness and exercise supervision.

Dunn-Coetzee (2015) found that there is very little efforts made in creating awareness in educating adolescents on internet usage in the context of South Africa, which led to the introduction of the phscho-educational strategy tool to educate South African adolescents. This tool is said to be a means to aid parents in educating their children. Dunn-Coetzee had structured questionnares completed by the adoloscents as part of the pre-limenary work. Some of the concerning results that came from the exercise was that there were some notable percentages of adoloscents who admtted to sharing their contact numbers, who shared their addresses and lied about their online activities to their parents.

These concerns emphasizes the need to educate children so that they are aware of the safe internet usage even when parents are physically not present with the children which speaks to the research conducted by Marais (2012).

The research conducted by Paraiso (2019) has also higlighted with reference to literature the lack of structured appraoches in South Africa to help parents gain knowledge and skills which will enable them to raise safety awareness on internet usage to their children. Paraiso also echoed previous researches which higlighted the frustration of parents on their inadequecy on digital literacy due to the rapid technology changes and inability to educate their children on cyber safety. Paraiso's literature review highlighted the lack of sufficent knowledge and material to aid in educating their children, particulary in the African context which includes South Africa,thus proposing the framework that should equip South African parents and enable them to educate their children on cyber saftey.

Kortjan and Von Solms (2013) conducted a comparative analysis amoungst different developed countries including United States of America (US), Canada, Australia and UK. The analysis conducted deduced different aims that each country has with their respective awareness and education initiatives. These included improving the level of awareness, supporting individuals through education, and fostering of cyber safety culture. Further to this, the analysis concluded that since the risks exposure is across all levels including both individuals and National levels of the society so is the need to afford education to all including parents and children. On their South African context, they deduced that South Africa is not prepared as a country to educate its citizen and thus they proposed a framework to help create a cyber safety culture amoungst all users.

### *2.4.2 Cyber Safety Resources*

From the research conducted by Paraiso (2019), literature review noted the different cyber safety formats which can be used to raise awareness which include presentation, websites, videos, interactive contents like games, books and newsletters.

Chadwick and Knight (2012) also echoed the internet risks which are exposed to pre-school children who are already starting to access computers. They shared some free online tools used in Australia which were introduced by the Australian Communication and Media Authority as part of their cybersafety education program called cybersmart. Some of the resources available included Cybersmart website which assists both parents and children in providing information on how to keep safe while online. It is highlighed that some of the content shared on the webste include current cybersecurity issues and practical ways of how to deal with them.

David et al. (2020) supported the notion of Mediation as one where, children's use of the internet is determined by rules which are set out to them, advices and discouragements they receive from other actors with parents being the main significant actors, whose responsibility is to protect the childen from internet risks due to their vulnerability. They higlighted two strategies of mediations, including active enabling mediation which entails the parental guidance practices which enables the children's positive use of the internet. Another mediation strategy was the restrictive mediation which limits the level or time of access or use of the internet thus reducing the amount of time children are exposed on the internet risks.

#### *2.4.3 Hypothesis 2*

The extent of parents communicating and educating their children on cyber safety influences the level of risks which children are exposed to.

## 2.5 Parents implementing proactive security measures and monitoring to monitor their children's online activities.

**Monitoring tools available**

As mentioned in the previous sections, as the technology evolves and new technologies are introduced, so are the cybersecurity risks landscape expanding.

Thus, it is important for parents to stay abreast of the different parental controls or monitoring technologies available that can help in monitoring their children's internet usage.

Technology industry has also been increasing the introduction of different software technologies to help parents keep their children safe from accessing inappropriate content, enabling early detection of cyberbullying, limiting online chats, and also preventing in-app purchases. Further to this, some monitoring software tools which are said to enable time restrictions, enable parents to also define allowed time slots for internet accesses. That way, the time spent by children on the internet is well managed. Those with content restrictions are said to be able to monitor both incoming and outgoing content. On the incoming content, the tools are able to do what is called whitelisting, which allows only pre-determines URLs to be accessed. The tools can also detect and block inappropriate age content like nudity and prevent children from uploading certain content on the internet like sharing of personal information or videos. Those with in-app purchase monitoring, enable parents to detect unwanted or unapproved in-game or pop-us online purchase activities. The settings would also enable the parent to configure according to the level of control required from default to maximum level based on their needs. From a reporting perspective, they are able to provide reports on the browser histories to help parents keep track on the type of websites their children are accessing (Zaman & Nouwen, 2016).

On the South African context, Kritzinger (2017) noted from her survey that although parents are making use the monitoring software, there is a higher percentage of parents not installing these software's than those who do and majority of the students who were surveyed confirmed that they have accessed inappropriate content. This shows that they are intentionally accessing these sites and there is no level of parent control on the type of content these children have access to.

On a research by Baldry, Sorrentino, and Farrington (2019), they needed to determine whether parental monitoring and supervision is associated with lowering cyberbullying and cybervictimization by boys or girls. The results reported higher involvement levels of cyberbullying by boys than girls and this

was without parental controls of their online activities or even education. Although, this research is not focusing on a particular gender, these are concerning results as they do show the need for parents' involvement in monitoring their children's internet activities. Multiple researches have highlighted boys being perpetrators of cyberbullying against others than girls (Calvete, Orue, Estévez, Villardón, & Padilla, 2010; C. Lee & Shin, 2017; Slonje & Smith, 2008; Walrave & Heirman, 2011). With monitoring in place, parents would be able to have some means of identifying such bullying behaviours to address and help the child while still in their early years and prevent them from becoming a problem to the society. For girls who are being victimised, parents would be able to quickly pick up such issues and get their children the necessary help needed.

### *2.5.1 Hypothesis 3*

The parents' application of security and monitoring measure on children's devices to monitor their online activities minimizes the children's exposure to online risks

## 2.6 ANALYTICAL FRAMEWORK

.

### *2.6.1 Theoretical Framework*

The two theoretical frameworks which this research study will be guided by are the family systems theory and parental mediation theory. The family systems theory notes that family structure plays a key role in the emotional and wellbeing of an individual, and also has an influence on the day-day living, with rules, beliefs and values that shapes the family member overtime (Pfeiffer & In-Albon, 2022). The emphasis of Family systems theory is on the "behaviour that takes place in a given moment of interaction between members of the family"(Johnson & Ray, 2016). Using the definitions of family from the research conducted by Burton and Jayakody (2001), a family can be defined as intact with two biological parents, single parent and can also include extended family networks who are blood or

non-blood related kins. In the case of cyber safety practices, literature shows that educating of children by parents on the cyber safety and risks is one of the important controls that they can have in place to protect their children from cybersecurity risks. This can be through day-day engagements where parents guide and educate children on the different risky online behaviours, inappropriate online content, what cyberbullying is etc. This encourages open and transparent communication between parents and children and proactively improves the children's awareness of such risks on a day-to-day basis. Wisniewski, Xu, Rosson, and Carroll (2017); Wisniewski, Xu, Rosson, Perkins, and Carroll (2016) have also applied the family systems theory in their research study where they investigated on how teens communicate with parents on the online risks. Both findings by Wisniewsk et al in 2016 and 2017 reveal that open and understanding communication between parents and children was the solution to help children become more aware and know how to respond to such risks.

The framework guiding this study also include parental mediation theory, which is said to have been introduced as a results of the negative impacts which the media have on children(Norman, Boer, Seydel, & Mullan, 2015). James and Kur (2020) highlighted the parental mediation theory as an interpersonal interaction between parents and children, which helps socialize to children on the use of technologies. Their research investigated the strategies used by parents as a way to mediate risky experiences by children on the digital media (internet) and the consequences of each. Their research noted the active mediation (*which entails parents discussing about the media content*), restrictive (*which involves putting rules on children' usage*), co-use (*which involves motivating children of the safety use while sharing the media device*) and technical mediation (*which entails making use of software tools to filter, block and monitor inappropriate content*). These were highlighted as the four important tools to minimize the risks exposed to children while using and accessing the digital media. Their research found that some parents lean towards the active and restrictive parental mediation and parents confirmed the strategies to successful in mediating risky experiences on their children. Rani and Shreshtha (2021) noted the emergence of technical mediation including application of filters and software which help limit the exposures of children to certain internet content. They also referred to previous

research done which highlighted the importance of parents using monitoring tools to track children internet activities, which monitor the browser history and emails sent. This helps parents to be aware of what their children are exposing themselves to so that they can give the necessary education and guidance and protect them from further risks exposures. The parental mediation strategies have shown to be a recommendable theory on multiple researches (Daud, Omar, Hassan, Bolong, & Teimouri, 2014; S.-J. Lee, 2013; UK, 2016), where its benefits have been shown to be evident in mediating risks on children's internet usage.

Guided by these theories, the research evaluates if there is correlation on the level of risks which children are exposed to and the extent to which parents are knowledgeable of the cyber risks. It also evaluates the correlation of the extent of communication and education of children on such risks by parents and the level of the children risk exposure. This speaks to family systems setup where parents educate their children on the cybersecurity risks where there's also engagements and guidance of how to safely use the internet. Parents share the knowledge which they have on cybersecurity risks with their children and certain safety behaviours are therefore influenced on children as they navigate and use the internet. The communication and education also speak to active mediation where parents converse with their children on the cybersecurity risks and safety practices therefore influencing safety internet usage and behaviours. The research also evaluates the correlation of the application of monitoring technologies and the level of children risks exposure, which helps in testing the technical mediation theory which will hypothesis being evaluated.

### *2.6.2 Conceptual Framework*

The level of knowledge of cybersecurity by parents influences level of cybersecurity risks exposure on children while they are on internet.

The extent of parents educating their children on cyber safety influences the level of risks which children are exposed to.

The parents' application of monitoring software on children's devices to monitor their online activities has an impact on the children's exposure to online risks

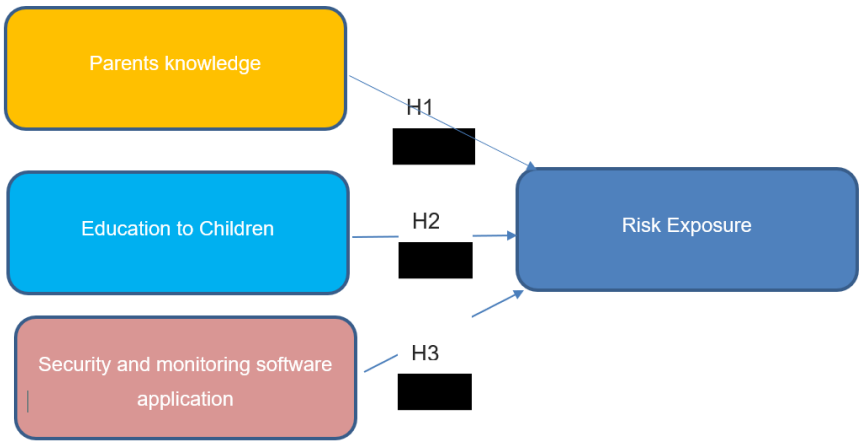



**Figure 1: Conceptual Framework**

## 2.7 Conclusion of Literature Review

The literature review conducted supports the notion of the need for continuous revisitation of cybersecurity awareness and knowledge amongst parents. Thus, to enable them to educate, monitor their children's internet usage activities to help minimize the risks exposure.

The theories guiding this research, which are the family systems theory and parental mediation theory have been proven from other studies, to be the guiding principles of investigations of cyber security awareness discussion where parents and children are involved which are in the context of family structures.

Based on literature conducted, the following hypotheses were deduced:

*2.7.1 H1: The level of knowledge of cybersecurity by parents influences level of cybersecurity risks exposure on children while they are on internet.*

*2.7.2 H2: The extent of parents educating their children on cyber safety influences the level of risks which children are exposed to.*

*2.7.3 H3: The parents' application of security settings and monitoring software on children' devices to protect them and monitor their online activities has an impact on the children's exposure to online risks.*

# CHAPTER 3. RESEARCH METHODOLOGY

This chapter describes the research approach, design and methods employed to collect the data. The population, sample and research instrument is introduced together with data collection procedure, analysis strategy and limitations. Finally, the quality assurance processes are described.

The research investigates South African parents' level of cybersecurity awareness and knowledge of cybersecurity risks which impact children; the extent to which parents are educating children of safety practices; and the extent to which they are implementing proactive security measures and monitoring to monitors children's online activities. The knowledge of parents, parents to child education and the proactive monitoring measures are the identified independent variables which will help on the study to determine and measure the level of awareness as the outcome of the investigation.

John W. (2009) in his research design book noted that:

> Quantitative research is a means for testing objectives theories by examining the relationship among variables. These variables in turn, can be measured, typically on instruments, so that the number data can be analysed using statistical procedure. (p. 48)

This research applies quantitative methods in order to answer the research questions identified. It evaluates the level of influence which the three independent variables have on the outcome or dependent variable which is the risk exposure of children.

The quantitative method is most appropriate for this study due to the focus on investigating the relationships between variables with the post positivist lens, The post positivist lens aims to observe and measure objectively the reality of the theories defined with the focus mainly on the human being views of the world and its meaning is based on historical and social perspectives (John W., 2009).

The study also seeks to generalise the results based on the on the statistical data collected, which is not in line with the qualitative type of a study that focuses on

understanding a phenomenon based on participant's views. Thus, quantitative research method was opted for.

## 3.1 Research design

This study adopts an online cross-sectional survey design to determine a general perception of the parents' awareness based on their responses to the closed-ended and/or guided questions. The online option allows the study to target a larger population of respondents, as it is not physically constrained. The survey was distributed at a point in time and only once. A longitudinal study would have compromised the completion time of the field work on data collection. Disadvantages of an online survey include non-responsiveness by respondents, To mitigate this courtesy reminder emails were distributed at regular intervals during the data collection process.

## 3.2 Data collection methods

John W. (2009) highlighted that a survey research method in quantitative study is to generalise from a sample of a population in order to make a conclusion about characteristics, attitude or behaviour of a population. This study used a self-administered survey questionnaire, using the online channel to enable the researcher to have access to the targeted population. The survey allowed participants to respond to the questionnaire anonymously and allowed them to take as much time to complete without any fear of prejudice. The online channels used were emails and WhatsApp groups.

## 3.3 Population and sample

### *3.3.1 Population*

The population targeted for the study were parents of children between the age of 3 and 12, who live with their children in the household and are accessible via email and social media platforms.

### *3.3.2 Sample and Sample Method*

The sample consists of parents or guardians that have children between the ages of 3 and 12 years, who live with their children in their households.

A total of 144 participants responded to the survey questionnaire and 83 responses were received which qualified the sample required of ages between 3 and 12 years. The research used random and snowballing sampling techniques. Random sampling technique was applied by randomly sending the survey invites to a database of 200 members in a church community via email. More invites were sent to WhatsApp group members in an estate in Pretoria and also the researchers contacts of 500 members. The sampling allowed an equal chance of completing the sample on the selected population (Etikan & Bala). Thus, survey was sent to everyone in the targeted groups. Snowballing technique was used in order to get as many participations from the public as possible, by requesting participants to forward the survey to their networks for them to also participate and complete survey.

## 3.4 The research instrument.

The study employed a self-compiled questionnaire which emerged from the literature review. Self-compilation of the questionnaire has been opted to help answer questions specific to the context of this research and its literature.

The Qualtrics software tool was used to create the online survey questionnaire and to collect responses.

The research instrument consisted of 12 questions, with a level of measurement at a nominal or an ordinal level. The questionnaire was divided into 4 sections which measured various themes:

A Demographic data

B Parents' knowledgeability on cybersecurity risks

C Parents educating children on cybersecurity risks

D Parents implementing proactive security measures

Data that was collected from the survey was analysed using SPSS version 28.0 tool. The results which will be presented in the next chapter is descriptive statistics are in the form of graphs, cross tabulations and other figures for the quantitative data collected. Inferential statistical techniques included the use of correlations and chi square test values, interpreted using the p-values. The traditional approach requires a statement of statistical significance to reporting, which is indicated by "$p < 0.05$".

## 3.5 Procedure for data collection

The survey instrument was peer reviewed in order to determine if there are any recommendations on improvements prior to sending out the survey questionnaires to the rest of the participants. Five participants were identified, and no changes were recommended on the survey questionnaires.

Following that, the survey was piloted in December 2022 to evaluate the feasibility of the research study and gauge the responsiveness of the participants.

The survey was distributed to the participants in January 2023, also applying the snowball sampling. The survey questionnaire was sent to a total of about 700 participants via email and through WhatsApp groups.

Survey participation letter sent out as part of the distribution included an overview of the research to provide the participant with context of the survey.

## 3.6 Data analysis strategies and interpretation

Ong and Puteh (2017) shared the different statistical analysis methods, including the univariate and multivariate comparison analysis and the bivariate and multivariate correlation statistical analysis.

This study applies multivariate correlation statistical analysis method which uses the multiple linear regression (MLR) analysis, which involves examining the causal and effect relationship of more than one independent variables which are paired against one dependent variable (Ong & Puteh, 2017).

The study intends to examine reaction of the three independent variables identified on the hypothesis (i.e., knowledge of parents, education to child by parents and proactive security measures and monitoring application one dependent variable) have a high, medium, or low impact on the risk exposure of the children to the cybersecurity risks.

Factor analysis was used for the data reduction. As highlighted by Shrestha (2021), it is suitable for reduction of extraction from a large number of related variables to few factors prior to using them for other analysis such as multivariate analysis.

The matrix table below is preceded by a summarised table which reflects the results of Kaiser-Meyer-Olkin (KMO) and Bartlett's Tests. These are the test conditions for factor analysis.

Shrestha (2021) further explained KMO as a measure of data suitability for factor analysis which tests adequacy of the sample size. Bartlett test was explained as a sphericity test, which tests the hypothesis that the correlation matrix is an identity matrix, which would indicate that the variables are unrelated and therefore unsuitable for structure detection. For the KMO, the measuring value is said to vary from 0 and 1 and if it is less than 0.5, the results of the factor analysis will not be suitable for data analysis. For Bartlett’s test, the significant value should be less than 0.05.

**KMO and Bartlett's Test:**

**Table 1: KMO and Bartlett test**

| | Section | Kaiser-Meyer-Olkin Measure of Sampling Adequacy | Bartlett's Test of Sphericity | | |
|---|---|---|---|---|---|
| | | | Approx. Chi-Square | df | Sig. |
| B | All items | 0.787 | 1078.026 | 231 | < 0.001 |

As highlighted on the above table 1, all the conditions are satisfactory for factor analysis.

**Table 2: Rotated Component Matrix**

**Rotated Component Matrix[a]**

| | Component | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | |
| I am able to work on a computer | 0,174 | -0,242 | 0,831 | mpuser_usag |
| I am able to interact via online social media platforms? | 0,075 | 0,073 | 0,886 | nline_platform |
| Cyberbullying | 0,213 | 0,728 | 0,119 | berbullying_ri |
| Cyberstalking | 0,052 | 0,850 | 0,086 | berstalking_ri |
| Stranger danger | 0,054 | 0,604 | 0,016 | nger_danger_ |
| Identify scam | -0,018 | 0,759 | 0,134 | ntity_scam_r Knowledge |
| Phishing scam | -0,009 | 0,760 | -0,139 | hing_scam_ |
| Online Gaming | 0,247 | 0,627 | 0,518 | _gaming_ser |
| Chat groups | 0,087 | 0,582 | 0,661 | _group_servi |
| Instagram, Facebook, Tik Tok, Twitter etc | 0,096 | 0,447 | 0,759 | l_media_ser |
| Ecommerce platforms | 0,247 | 0,642 | 0,399 | mmerce_serv |
| I actively talk to my child about internet use | 0,765 | -0,027 | 0,082 | internet_talk |
| I teach my child to keep personal information private (e.g. not share phone numbers, addresses, credit card info etc) | 0,651 | 0,018 | 0,000 | personal_info Education |
| I encourage my child to come to me if they encounter a problem while online (e.g. being bullied, getting directed to inappropriate sites etc) | 0,712 | -0,021 | 0,172 | blems_encou |
| Firewall | 0,708 | 0,416 | 0,143 | firewall_aware |
| Spam blocker | 0,611 | 0,507 | 0,167 | m_blocker_av |
| Filtering software | 0,686 | 0,477 | 0,075 | _software_av |
| Time limiting software | 0,619 | 0,524 | -0,031 | mit_software_ Security |
| Monitoring Software | 0,783 | 0,433 | 0,131 | ring_software |
| Online purchase payment passwords | 0,628 | -0,141 | 0,083 | ay_password |
| I have applied practical measures to protect my child while online (e.g. change passwords, apply browser filters, anti-virus, spam blocker etc)? | 0,832 | 0,061 | 0,029 | security_me |
| I actively monitor my child's online activity (e.g. Check browser history, Check online account, Messages, Contacts) | 0,682 | 0,121 | 0,096 | e_activity_tra |

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 5 iterations.

Referencing the above table 2, the principal component analysis was used as the extraction method, and the rotation method was Varimax with Kaiser Normalization. This is an orthogonal rotation method that minimizes the number of variables that have high loadings on each factor and it simplifies the interpretation of the factors. Factor analysis/loading show inter-correlations between variables.

Items of questions that loaded similarly imply measurement along a similar factor. An examination of the content of items loading at or above 0.5 (and using the higher or highest loading in instances where items cross-loaded at greater than this value) effectively measured along the various components.

The statements that constituted Education and Security loaded perfectly along a single component. This implies that the statements that constituted these sections perfectly measured what it set out to measure.

It is noted that the variables that constituted Section on Knowledge loaded along 2 components (sub-themes), with the sub-section (Q5) aligning perfectly. This means that respondents identified different trends within the section. Within the section, the splits are colour coded.

## 3.7 Possible limitations and challenges of the study

The quantitative research method used close-ended and guided questions to get input from participants. There might have been a lot more input or context that can be attained from participants if open-ended questions are also included during the data collection. Therefore, complementing the quantitative with qualitative questions could have enabled the researchers to do a deeper analysis and interpretation of data.

## 3.8 Quality Assurance

### *3.8.1 External validity*

Campbell and Stanley (2015) shared the threats of external validity including the interaction effect of testing, in which the pre-testing experiments variables can result to an increase or decrease in the participants responsiveness. Although this study has pre-testing (i.e., pilot test) conducted, it is a first time for all participants as the survey was not redistributed on participants who formed part of the pilot test. Another threat highlighted was the interaction of selection bias effect, in which bias effect can occur due to familiarity of the participants with the researcher which can affect the generalizability. For the study to address this threat, anonymity was enforced with no name or surname of the participants required on the survey questions. It was clearly declared as part of the survey introduction that the participants responses will be kept anonymous.

The study sample was deliberately diversified to ensure it covers a broader range of the population thus creating more generalizability.

### *3.8.2 Internal validity*

The study has adopted a quantitative and cross-sectional survey design therefore addressing the follow threats (John W., 2009):

- Instrumentation effect as only one instrument (which Is the survey questionnaire) at point in time will be used to collect data.
- Testing effect, where participants can become familiar with questions on the second run.
- History effect, where unduly events can occurs influencing the outcome.

Random sampling, to enable even and equal probability of participants being selected for the survey and broader sampling of the population through selecting different participants demographics will also address selection threat effect of the internal validity.

### *3.8.3 Reliability*

Golafshani (2003) highlighted the importance of ensuring consistency and accuracy on the tests and scores as those are the measures for reliability of the as shown from previous studies. The survey questions for this study have been defined with consistent measurements scoring, which is using the 5 Likert scale across the survey questionnaire. Therefore, the survey should be replicable if run with a different sample or population.

## 3.9 Ethical considerations

As part of the data collection process, this research followed the guidelines applicable as follows. A request for permission to get parents of the school to participate on the survey was sent to the school principal which was declined due to their policy restrictions. The Head Pastor formally approved the collection of

the survey data from church members by sending the survey via their internal email and WhatsApp groups.

The participants information sheet was shared as the cover pages of the actual survey questionnaire which explain what the survey is about and all the relevant information about the survey.

# CHAPTER 4. PRESENTATION OF RESULTS

## 4.1 Introduction

This chapter presents the results and discuss the findings on the collected data from survey questionnaires distributed to the participants. The questionnaire was the primary tool that was used to collect data and was distributed to parents who have online access via emails and WhatsApp messaging. The results have been presented per Hypothesis and also an overall summary has also been presented.

In total, 700 questionnaires were dispatched and 144 responses were received with 83 which returned with a Y% response rate.

The two most important aspects of precision which are reliability and validity were applied. A reliability coefficient of 0.60 or higher is considered as “acceptable” for a newly developed construct.

The table below reflects the Cronbach’s alpha score for all the items that constituted the questionnaire.

**Table 3: Questionnaire sections**

| | Section | Number of Items | Cronbach's Alpha |
|---|---|---|---|
| Q3 - Q6 | Knowledge | 10 | 0.893 |
| Q7 - Q9 | Education | 3 | 0.884 |
| Q10 - Q12 | Security | 8 | 0.919 |
| All items included | | 22 | 0.918 |

The reliability scores for all sections exceed the recommended Cronbach’s alpha value. This indicated a degree of acceptable and consistent scoring for the sections of the research.

The section that follows analysed the scoring patterns of the respondents per variable per section.
The results were first presented using summarised percentages for the variables that constitute each section.

## 4.2 Results and discussion pertaining to Hypothesis 1

In relation to Hypothesis 1 which refers to the level of knowledgeability of cybersecurity risks which influence the risk exposure, the following results present the parents awareness and knowledgeability of cybersecurity risks and whether they are able to use the tools needed to access the internet.

The results are linked to the research in that without the awareness, knowledge of the risks or any ability to use the tools used to access the internet, parents will not be able to protect their children that connect to the internet.

The table below reflected the scoring related to “I am able to work on a computer”.

**Table 4: Ability to use computers (%)**

| Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | Strongly Agree | | Chi Square p-value | |
|---|---|---|---|---|---|---|---|---|---|---|
| Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| 3 | 3.6% | 0 | 0.0% | 0 | 0.0% | 7 | 8.4% | 73 | 88.0% | < 0.001 |

A significant proportion of the respondents agreed with the statement (96.4%).
The next table below shows the responses to “I am able to interact via online social media platforms”.

**Table 5: Ability to Navigate on social media platforms (%)**

| Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | Strongly Agree | | Chi Square p-value | |
|---|---|---|---|---|---|---|---|---|---|---|
| Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| 3 | 3.6% | 0 | 0.0% | 1 | 1.2% | 6 | 7.2% | 73 | 88.0% | < 0.001 |

A significant also proportion of the respondents agreed with the statement (95.2%).

The table below summarised the scoring patterns for the respondes to " I am aware and knowledgeable on these cybersecurity risks".

**Table 6: Awareness and knowledge on cybersecurity risks**

| | | Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | | Strongly Agree | | Chi Square p-value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| Cyberbullying | Q5.1 | 1 | 1.2% | 2 | 2.4% | 3 | 3.7% | 16 | 19.5 % | 60 | 73.2 % | < 0.001 |
| Cyberstalking | Q5.2 | 3 | 3.7% | 2 | 2.5% | 6 | 7.4% | 22 | 27.2 % | 48 | 59.3 % | < 0.001 |
| Stranger danger | Q5.3 | 2 | 2.5% | 6 | 7.5% | 1 | 1.3% | 18 | 22.5 % | 53 | 66.3 % | < 0.001 |
| Identify scam | Q5.4 | 1 | 1.3% | 3 | 3.8% | 5 | 6.3% | 21 | 26.3 % | 50 | 62.5 % | < 0.001 |
| Phishing scam | Q5.5 | 3 | 3.7% | 4 | 4.9% | 7 | 8.6% | 19 | 23.5 % | 48 | 59.3 % | < 0.001 |

The following patterns were observed:

- All statements showed (significantly) higher levels of agreement whilst other levels of agreement were lower (but still greater than levels of disagreement)
- There were no statements with higher levels of disagreement
- The significance of the differences was tested and shown in the table.

The final table below for this section summarised the scoring patterns for the responses to " I am aware and knowledgeable of the potential risks faced on the following internet services"

**Table 7: Awareness and knowledge of potential risks faced on online services.**

| | | Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | | Strongly Agree | | Chi Square p-value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| Online Gaming | Q6.1 | 6 | 7.5% | 2 | 2.5% | 3 | 3.8% | 19 | 23.8% | 50 | 62.5% | < 0.001 |
| Chat groups | Q6.2 | 4 | 5.0% | 3 | 3.8% | 3 | 3.8% | 19 | 23.8% | 51 | 63.8% | < 0.001 |
| Instagram, Facebook, Tik Tok, Twitter etc | Q6.3 | 3 | 3.6% | 1 | 1.2% | 2 | 2.4% | 17 | 20.5% | 60 | 72.3% | < 0.001 |
| Ecommerce platforms | Q6.4 | 4 | 4.8% | 2 | 2.4% | 8 | 9.6% | 20 | 24.1% | 49 | 59.0% | < 0.001 |

The following patterns were observed:

- All statements on this question also showed (significantly) higher levels of agreement whilst other levels of agreement were lower (but still greater than levels of disagreement)
- There were also no statements with higher levels of disagreement
- The significance of the differences was also tested and shown in the table.

The overall results found notably higher agreement levels for parents who were aware and knowledgeable of cyberbullying risks and those who were aware of potential risks faced on social media platform services. These findings were not in agreement with the previous findings from literature.

In the research conducted by Kritzinger (2017), it was found that there was lack of parents' knowledge and confidence in addressing risks related to cybersecurity which in turn can result to children being bullied while online. The same concern was also raised from a research by Mariska (2012) on her research about the guidelines to establish e-safety awareness. Kortjan and Von Solms (2014) also highlighted similar lack of parents' knowledge because of government lack on involvement in driving education initiatives.

The results have also shown notably high agreement levels on the use of computers and ability to navigate on the online social media platforms. These

would put parents in a better position on facilitating the protection of children since they have good understanding of the tools which their children are making use of and they are aware and knowledgeable of the risks children are exposed to. Theoretical framework touched on the concept of mediation theory on co-use. With parents co-using the same tools or devices which their children use when accessing the internet, it gives a better chance for the parents to get visibility of the same risks which are exposed to their children which in turn allows them to be more involved in motivating their children of the safety use.

## 4.3 Results and discussion pertaining to Hypothesis 2

This section dealt with the extent which parents educating their children on the cybersecurity risks have on children' exposure to such risks.

The table below summarised the scoring patterns of parents educating their children about cybersecurity risks.

**Table 8: Parents educating their children.**

| | | Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | | Strongly Agree | | Chi Square p-value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| I actively talk to my child about internet use | Q7 | 10 | 12.2% | 5 | 6.1% | 7 | 8.5% | 28 | 34.1% | 32 | 39.0% | < 0.001 |
| I teach my child to keep personal information private (e.g., not share phone numbers, addresses, credit card info etc) | Q8 | 6 | 7.2% | 7 | 8.4% | 13 | 15.7% | 15 | 18.1% | 42 | 50.6% | < 0.001 |
| I encourage my child to come to me if they encounter a problem while online (e.g., being bullied, getting directed to inappropriate sites etc) | Q9 | 7 | 8.4% | 6 | 7.2% | 9 | 10.8% | 14 | 16.9% | 47 | 56.6% | < 0.001 |

Patterns observed notably lower levels compared to the results related to hypothesis 1. However, the respondents who were in agreement and were

educating children on the cybersecurity risks, still reflected higher than those who did not agree. The lowest patterns observed where on parents who teach their children to keep personal information private which was at 68,7% and the highest was at 73,5% for parents who encourage their child to come to them if the encounter a problem online.

Literature has noted the need to educate children as the days of physical supervision have passed and children are able to even bypass the online restrictions while accessing the internet. Therefore teaching them safety practices plays a vital role in ensuring that they are protected Marais (2012),

Previous research has identified the lack of parents educating children as a concern.

Dunn-Coetzee (2015) developed and introduced a tool as part the research to help parents to educate their children as a result of the observed lack or little efforts made by parents. Similarly, Kortjan and Von Solms (2013) observed the unpreparedness of South African parents in ensuring children safety which led to a proposal a framework is the attempt to aid parents to educate their children.

The results observed on this study regarding parents educating children have shown to agree with the previous research in that there was still a need for improvement.

In relation to the theoretical framework, family system theory has noted that, family structure plays an important role on influencing day to day living with rules, values and believes. In terms of this results, it would appear that though parents in the respondent's family structures were knowledgeable of the cybersecurity risks, they were not influencing the safe practices of using the internet which would be done through educating the child.

Regarding the parental mediation framework, which highlighted the interpersonal interaction between parents and children which included active mediation and technical mediation, the results showed that parents were not socialising and creating awareness of such risks to teach safe use of the internet to their children. These were observed by the lower patterns on parents who teach their children

to keep personal information private which was at 68,7%, those who actively talk to their children which was at 73,1 % and the highest was for those who encourage their children to engage them if they encounter a problem, for example if they were bullied, which was at 73,5%.

## 4.4 Results and discussion pertaining to Hypothesis 3

This section dealt with the patterns of parents who applied security and monitoring measures in order to minimize the risk exposure on children while accessing the internet.

The table below summarised the scoring patterns.

**Table 9: Security and monitoring measures**

| | | Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | | Strongly Agree | | Chi Square p-value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| Firewall | Q10.1 | 7 | 8.6% | 8 | 9.9% | 7 | 8.6% | 20 | 24.7 % | 39 | 48.1 % | < 0.001 |
| Spam blocker | Q10.2 | 7 | 8.5% | 7 | 8.5% | 5 | 6.1% | 20 | 24.4 % | 43 | 52.4 % | < 0.001 |
| Filtering software | Q10.3 | 13 | 16.0 % | 9 | 11.1 % | 15 | 18.5 % | 15 | 18.5 % | 29 | 35.8 % | 0.007 |
| Time limiting software | Q10.4 | 8 | 10.5 % | 11 | 14.5 % | 14 | 18.4 % | 14 | 18.4 % | 29 | 38.2 % | 0.002 |
| Monitoring Software | Q10.5 | 11 | 13.8 % | 10 | 12.5 % | 9 | 11.3 % | 15 | 18.8 % | 35 | 43.8 % | < 0.001 |
| Online purchase payment passwords | Q10.6 | 5 | 6.4% | 2 | 2.6% | 9 | 11.5 % | 9 | 11.5 % | 53 | 67.9 % | < 0.001 |

Similar to the results from hypothesis 2 which dealt with the parents educating children on the risks, the patterns for awareness of security measures were also notably lower. The highest level of parents who were in agreement where parents aware of online purchase payment passwords which was at 79,4% and the lowest was reported at 54,3 % for parents who were aware of filtering software.

The table below indicates the scoring for “I have applied practical measures to protect my child while online (e.g., change passwords, apply browser filters, anti-virus, spam blocker etc)”.

**Table 10: Application of security measures**

| Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | | Strongly Agree | | Chi Square p-value |
|---|---|---|---|---|---|---|---|---|---|---|
| Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| 8 | 10.0% | 7 | 8.8% | 12 | 15.0% | 23 | 28.8% | 30 | 37.5% | < 0.001 |

Two thirds of the respondents (66.3%) agreed that they have taken practical steps to protect their children online. Of the remaining third, approximately half of the respondents each disagreed or were neutral.

The responses to “I actively monitor my child’s online activity (e.g., Check browser history, check online account, Messages, Contacts)” is shown in the table below.

**Table 11: Active monitoring**

| Strongly Disagree | | Somewhat disagree | | Neither agree nor disagree | | Somewhat agree | | Strongly Agree | | Chi Square p-value |
|---|---|---|---|---|---|---|---|---|---|---|
| Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | Count | Row N % | |
| 8 | 9.8% | 4 | 4.9% | 10 | 12.2% | 17 | 20.7% | 43 | 52.4% | < 0.001 |

Approximately three-quarters of the respondents (73.1%) agreed that they actively monitored their children’s online activities, with similar numbers of respondents disagreeing or not having an opinion.

As literature has highlighted, it is imperative for parents to keep abreast of the different parental controls and monitoring technologies since the technology world is changing constantly. This is to help in facilitating the protection of children who are not able to protect themselves.

In a study conducted by Kritzinger (2017), it was noted that although there are parents who are aware of the security technologies and are implementing them, there was still a higher percentage of those who do not implement the technologies therefore exposing children to inappropriate content on the internet.

Further to this, Kritzinger also noted of children having access to and own cell phones and do not need constant permission from parents to use and therefore access the internet anytime. A noticeable percentage of parents were highlighted as not monitoring their children internet activities.

An article titled “Cyber Risks Awaiting Children and Young People in the 21st Century” (2022) also noted of long hours that children spend on the internet and social media which have opportunities of getting children to develop negative emotions such depression and low self-esteem etc. The article also highlighted cyberbullying being one of the major risks facing children on the internet. Therefore If children are spending such long hours on the internet and no form of security measures, the probability of them getting exposed and exploited are therefore increased.

With regards to the theoretical framework, technical mediation was noted as an important tool which entails making use of software tools to filter, block and monitor inappropriate content. The results as depicted on the tables highlighted a need for further improvement when it comes to parents’ application of security measures in order to protect children when accessing the internet.

## 4.5 Summary of the results and findings

Having looked at the results of the parents’ knowledge for cybersecurity risks, parents educating children on the risks and application of security and monitoring measures, the awareness and knowledge of cybersecurity risks was notably high and the other two noted a need for further improvement..

In relation to the conceptual theory, parents’ knowledge and awareness of cybersecurity risks, parents educating children on the risks and applying security

measures have a direct impact on the risk exposure of children on the internet. With just parents that have the awareness and knowledge of the risks without passing on that knowledge by educating them on the safety practices of using the internet and also applying security measures on the devices they use, the risk exposure still remains.

### 4.5.1. Crosstabulations

A Chi square test of independence was performed to determine whether there was a statistically significant relationship between the variables (rows vs columns). The null hypothesis states that there is no association between the two. The alternate hypothesis indicates that there is an association.

The table summarised the results of the chi square tests. Refer to appendix E on the Crosstabs.

As an example, this implies that respondents that are aware and knowledgeable about of cyberbullying would educate their children on the risks and also apply the security and monitoring measures.

### 4.5.2. Correlations

Bivariate correlation was also performed on the (ordinal) data. The results are found in the appendix F.
The results indicate the following patterns.
Positive values indicate a directly proportional relationship between the variables and a negative value indicates an inverse relationship. All significant relationships are indicated by a * or **.

For example, the correlation value between “Cyberbullying” and “Filtering software” is 0,504**. This is directly related proportionality. Respondents indicate that the greater the evidence of knowledge of cyberbullying, the more

likely they would be to use filtering software, and vice versa. As a result, reducing the risk exposure on the children.

### 4.5.3. Structural equation model

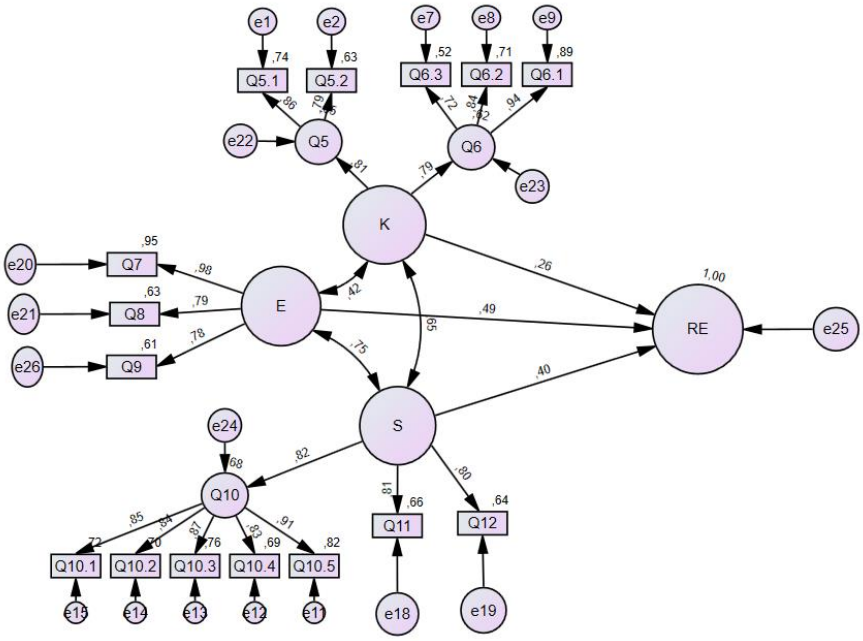



**Figure 2: Modified SEM**

The model is a multivariate statistical result that was obtained using structural relationships, applying a combination of factor analysis and multiple regression analysis techniques. It is used to analyse the structural relationship between measured variables and latent constructs.

The dimensions are coded as under reliability.

Minimum was achieved.
Chi-square = 166,223
Degrees of freedom = 86
Probability level = ,000

This Chi-square tests the null hypothesis that the overidentified (reduced) model fits the data as well as does a just-identified (full, saturated) model. In a just-identified model there is a direct path (not through an intervening variable) from each variable to each other variable. In such a model the Chi-square will always have a value of zero, since the fit will always be perfect. The probability should **not** be significant. In this model, the chi square p-value is < 0.050 (p = 0.005).

It is however worth noting that even though, technically, the Chi-Square should be non-significant in model testing, this is very hard to achieve due to the usually large sample required for it. Hence, if it is in fact significant, that isn't a problem so long as the other indicators of fit are good.

**Maximum Likelihood Estimates**

**Regression Weights: (Group number 1 - Default model)**

| | | | Estimate | S.E. | C.R. | P | Label |
|---|---|---|---|---|---|---|---|
| Q5 | <--- | K | ,823 | ,205 | 4,015 | *** | par_7 |
| Q10 | <--- | S | ,989 | ,128 | 7,738 | *** | par_8 |
| Q6 | <--- | K | 1,000 | | | | |
| Q5.1 | <--- | Q5 | 1,000 | | | | |
| Q5.2 | <--- | Q5 | 1,000 | | | | |
| Q6.3 | <--- | Q6 | ,724 | ,099 | 7,335 | *** | par_1 |
| Q6.2 | <--- | Q6 | 1,000 | | | | |
| Q6.1 | <--- | Q6 | 1,216 | ,125 | 9,711 | *** | par_2 |
| Q10.5 | <--- | Q10 | 1,039 | ,090 | 11,589 | *** | par_3 |
| Q10.4 | <--- | Q10 | ,899 | ,094 | 9,565 | *** | par_4 |
| Q10.3 | <--- | Q10 | 1,000 | | | | |
| Q10.2 | <--- | Q10 | ,848 | ,085 | 9,935 | *** | par_5 |
| Q10.1 | <--- | Q10 | ,873 | ,085 | 10,212 | *** | par_6 |
| Q11 | <--- | S | 1,000 | | | | |
| Q7 | <--- | E | 1,000 | | | | |
| Q8 | <--- | E | ,778 | ,080 | 9,737 | *** | par_9 |
| Q12 | <--- | S | 1,000 | | | | |
| RE | <--- | K | 1,000 | | | | |
| RE | <--- | E | 1,000 | | | | |
| RE | <--- | S | 1,000 | | | | |
| Q9 | <--- | E | ,788 | ,082 | 9,587 | *** | par_13 |

The variables loaded strongly along their various factors (significant p-values indicated by *** p < 0.001). These verify the EFA obtained under factor analysis.

**Standardized Regression Weights: (Group number 1 - Default model)**

| | | | Estimate |
|---|---|---|---|
| Q5 | <--- | K | ,808 |
| Q10 | <--- | S | ,825 |
| Q6 | <--- | K | ,790 |
| Q5.1 | <--- | Q5 | ,861 |
| Q5.2 | <--- | Q5 | ,795 |
| Q6.3 | <--- | Q6 | ,720 |
| Q6.2 | <--- | Q6 | ,842 |
| Q6.1 | <--- | Q6 | ,944 |
| Q10.5 | <--- | Q10 | ,906 |
| Q10.4 | <--- | Q10 | ,829 |
| Q10.3 | <--- | Q10 | ,874 |
| Q10.2 | <--- | Q10 | ,835 |
| Q10.1 | <--- | Q10 | ,848 |
| Q11 | <--- | S | ,815 |
| Q7 | <--- | E | ,977 |
| Q8 | <--- | E | ,791 |
| Q12 | <--- | S | ,798 |
| RE | <--- | K | ,263 |
| RE | <--- | E | ,488 |
| RE | <--- | S | ,399 |
| Q9 | <--- | E | ,784 |

The parameters are estimated by maximum likelihood (ML) methods, which (is an iterative procedure that) attempts to maximize the likelihood that obtained values of the criterion variable will be correctly predicted. All of the coefficients were above the suggested value of 0.600. Statements that loaded poorly or that were redundant were omitted from the model.

**Model Fit Summary**

The suggested acceptable value for relative chi-square, CMIN/DF should not be greater than 5 which are used to reduce dependency on sample size. However, the cut-off points for TLI, CFI, NFI and IFI is between zero to one. A good model is indicated by RMSEA value of less than or equal to 0.05.

**CMIN**

| Model | NPAR | CMIN | DF | P | CMIN/DF |
|---|---|---|---|---|---|
| **Default model** | 49 | 166,223 | 86 | ,000 | 1,913 |
| **Saturated model** | 135 | ,000 | 0 | | |
| **Independence model** | 15 | 1011,574 | 120 | ,000 | 8,430 |

CMIN is a Chi-square statistic comparing the tested model and the independence model to the saturated model. The ratio, CMIN/DF, the relative chi-square, is an index of how much the fit of data to model has been reduced by dropping one or more paths. The CMIN/DF is less than the acceptable value of 5 (1.913). This meets the CMIN condition.

**Baseline Comparisons**

| Model | NFI Delta1 | RFI rho1 | IFI Delta2 | TLI rho2 | CFI |
|---|---|---|---|---|---|
| **Default model** | ,836 | ,771 | ,913 | ,874 | ,910 |

For this data, the NFI is 0.836, which is marginally less than the recommended value of 0.90 for a good fit. The Comparative Fit Index (CFI) uses a similar approach (with a noncentral chi-square) and is said to be a good index for use even with small samples. It ranges from 0 to 1, like the NFI, and 0.90 indicates good fit. The CFI value is 0.910, implying a good fit.

**Regression Analysis**

The level of significance relates to the strength of the relationships. The correlations are tested below.

Covariances: (Group number 1 - Default model)

| | | | Estimate | S.E. | C.R. | P | Label |
|---|---|---|---|---|---|---|---|
| E | <--> | K | ,384 | ,140 | 2,747 | ,006 | par_10 |
| K | <--> | S | ,488 | ,138 | 3,538 | *** | par_11 |

| | | | Estimate | S.E. | C.R. | P | Label |
|---|---|---|---|---|---|---|---|
| E | <--> | S | 1,038 | ,210 | 4,936 | *** | par_12 |

Correlations: (Group number 1 - Default model)

| | | | Estimate |
|---|---|---|---|
| E | <--> | K | ,418 |
| K | <--> | S | ,650 |
| E | <--> | S | ,745 |

Null hypothesis: There is no correlation between each of the dimensions.

Alternate hypothesis: There is a significant correlation.

All relationships are significant ($p < 0.050$). The results indicate a strong, directly proportional relationship between the latent variables, with each of the *r* estimates being positive.

For example: the correlation between Education (E) and Security (S) is strongly positively correlated ($r = 0.745$, $p < 0.001$). This implies the more educated parents are, the more likely they would have security measures in place, and vice versa. And subsequent to that and also referencing the conceptual framework, education has the highest coefficient of 0.49, therefore a change is education would have the largest impact on Risk exposure, followed by Security and then education.

For this research, the chi-square value is 166,223 with 86 degrees of freedom, resulting in a very low probability level < 0.001. This indicates that the observed data deviates significantly from the estimated model. Typically, a non-significant chi-square value ($p > 0.05$) suggests a good fit, but in this case, the chi-square value is statistically significant.

In this case, the CFI value (0.910) indicates a reasonably good fit, as values above 0.90 are considered acceptable. The TLI value (0.874) also suggests a relatively good fit, with values above 0.90 indicating satisfactory fit. The RMSEA value (0.081) fall within the moderate range, where values between 0.05 and 0.10 are considered acceptable.

Some of the low loading factors (statements) were omitted from the model. An inspection of the coefficients for each latent variable indicated high factor loadings. In addition, the path coefficients are reflected on the diagram. All of the coefficients are positive (proportional relationship) between the latent variables.

As this was a newly developed construct, it is also expected that the structural relationships may not have fitted accurately. However, certain indices are met and the model is an adequate fit, and it is a recommendation that the model be revised in terms of the measured variables constituting the latent variables to improve factor loadings.

# CHAPTER 5. CONCLUSIONS & RECOMMENDATIONS

## 5.1 Introduction

This chapter will provide a close out of the study with the conclusions of the identified research questions, integrating them with the research results based on the three hypotheses. The chapter will also provide recommendations and futures research suggestions.

## 5.2 Conclusions regarding research question 1

**Question1:** To what extent are parents knowledgeable of the cybersecurity risks which can impact their children while accessing the internet?

The survey questionnaire asked parents to assess themselves on their knowledgeability of different cybersecurity risk terminologies and risks faced on different internet services, which can potentially impact their children while they are online i.e., as presented on figure 2 and 3. The questionnaire also needed to determine if parents have capabilities of using a computer and also accessing and interacting on social media platforms.

The survey results suggested that most parents were knowledgeable of the cybersecurity risks. Therefore, the extent would be more high level since those who showed complete confidence had the highest 73,2% for cyberbullying awareness and those with “somewhat” knowledge of the risks were highest at 27,2% and the rest were split between not knowledgeable at all to not sure (i.e. neither agree nor disagree). Although this paper was in contrast to the previous literature with regards to the knowledge levels which were notably high on this research paper, this research suggested that there were still some of the parents who were still not completely aware of the cyber risks and thus focus on improvement would still be of importance.

Regarding the ability to use computers and being able to navigate on the social media platforms, parents have also shown highly knowledgeable. Their knowledge on the use of computers and also navigation on the social media platforms is a good start in getting an idea of what their children are exposed to while online. It should trigger the importance of getting as much more knowledge on such risks in order to protect their children.

## 5.3 Conclusions regarding research question 2

**Question 2:** To what extent are parents educating their children on the safety practices while connected to the internet?

Research question 2 needed to assess the extent to which parents talk to their children about internet use, teach them about keeping private information private and encouraging their children to go to them if and when they encounter problems.

The results to answer the research question suggested that, the extent was notably low as illustrated by the levels of parents educating the children which had the highest percentage of only 56,6% across all the different measures of the survey questionnaire in the education section.

## 5.4 Conclusions regarding research question 3

**Question 3:** To what extent are parents implementing proactive security and monitoring measures to protect and monitor their children's online activities?

On this research section, assessment was on whether parents were aware of the different security and monitoring technologies, whether they applied practical measures in order to protect their children while online and whether they actively monitor their children's online activities. On the awareness of technologies, applying of security measures and also tracking activities, the extent at which parents where implementing proactive measures were found to be significantly low with the application of security measures at the highest of only 37,5% for those parents who are confidently applying them.

## 5.5 Recommendations

Although, the study used a limited sample of parents, the results deduced from the study has shown that parents awareness levels on cybersecurity risks are still notably low. More focus on sensitising parents and building interest for them to get more knowledge and getting equipped on cybersecurity is still a necessity including the following recommendations:

- Government department of communication and technology can initiate campaigns and push educational notifications on cybersecurity. This will help in sensitising parents on the changes happening on the cybersecurity space.
- Government can introduce policies which enforce network service providers to package firewall setup upon implementing routers in the households. This should at the least assist in protecting children accessing the internet at their household wifi connections.
- Government needs to work with schools, both private and public in order to have cybersecurity specific programmes to educate children.
- Parents need to limit or delay screen time and encourage physical activities. Since this study applies to children from the age of , these are children who have not started school and therefore there is no need to introduce them to technology early. For those who are already at school, limiting can help in ensuring less chances of them being exposed.
- For parents who don't have security measures in place, routinely logging into their children's devices and just checking the browsers and applications which their children have access to can help in making sure that they are accessing safe sites and they not communicating with strangers. Although this will be a reactive approach, there will be at least some level monitoring.

## 5.6 Suggestions for further research

The study used a very limited sample and therefore resulting to a very limited scope. Future research would need to broaden the population and the age range in order improve on the generalization of the south African parents' population.

Future study can also consider using a mixed method and use both quantitative and qualitative method. Because quantitative using straight forward and closed ended questions, feedback is limited and restricted. Qualitative method can help in getting more in-depth feedback from parents like getting feedback on their concerns with regards to cybersecurity topic.

Future research can also look at what progress has been made from a government perspective in terms cybersecurity programme initiatives for the general public and whether, South Africans are aware of those initiatives.

**Table 12: Consistency table: research question, hypothesis, data collection and data analysis**

| RQ # | | State Research Question | hyp # | State Hypothesis | Data collection detail | Data analysis method |
|---|---|---|---|---|---|---|
| 1 | | To what extent are parents knowledgeable of the cybersecurity risks which can impact their children while accessing the internet? | 1 | The level of knowledge of cybersecurity by parents influences the level of cybersecurity risks exposure on children while they are on the internet. | Questionnaire Likert statement<br>3-6 | Regression analysis |
| 2 | | To what extent are parents educating their children on the safety practices while | 2 | The extent of parents educating their children on cyber safety influences the | Questionnaire Likert statement<br>7-9 | Regression analysis |

| RQ # | | State Research Question | hyp # | State Hypothesis | Data collection detail | Data analysis method |
|---|---|---|---|---|---|---|
| | | connected to the internet? | | level of risks which children are exposed to. | | |
| 3 | | To what extent are parents implementing proactive security and monitoring measures to protect and monitor their children's online activities? | 3 | The parents' application of security settings and monitoring software on children' devices to protect them and monitor their online activities has an impact on the children's exposure to online risks | Questionnaire Likert statement<br>10-12 | Regression analysis |
| | | | | | | |

# REFERENCES


Africa, C. C. o. A. (2022). Chilren's Rights. Retrieved from https://www.concourt.org.za/index.php/children-s-rights

Africa, U. N. C. s. F.-U. S. (2022). One third of children in South Africa at risk of online violence, exploitation and abuse. . Retrieved from https://www.unicef.org/southafrica/press-releases/one-third-children-south-africa-risk-online-violence-exploitation-and-abuse

Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication, 35*(2), 485-498.

AlShabibi, A., & Al-Suqri, M. (2021). *Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace*.

Alwanain, M. I. (2021). How Do Children Interact with Phishing Attacks? *International Journal of Computer Science & Network Security, 21*(3), 127-133.

Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet: A study of Devon, UK. *Interactive Technology and Smart Education, 13*(2), 147-165.

Constitution of the Republic of South Africa, 1996 - Chapter 2: Bill of Rights, § #28 (1996).

Bacıoğlu, S. D. (2022). Cyber Risks Awaiting Children and Young People in the 21st Century. *Psikiyatride Guncel Yaklasimlar, 14*(1), 29-37.

Badillo-Urquiola, K., Smriti, D., McNally, B., Golub, E., Bonsignore, E., & Wisniewski, P. J. (2019). *Stranger Danger! Social Media App Features Co-designed with Children to Keep Them Safe Online*. Paper presented at the Proceedings of the 18th ACM International Conference on Interaction Design and Children, Boise, ID, USA. https://doi.org/10.1145/3311927.3323133

Baldry, A. C., Sorrentino, A., & Farrington, D. P. (2019). Cyberbullying and cybervictimization versus parental supervision, monitoring and control of adolescents' online activities. *Children and youth services review, 96*, 302-307. doi:10.1016/j.childyouth.2018.11.058

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., & Pensa, R. G. (2018). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies, 12*(4), 456-469.

Burton, L. M., & Jayakody, R. (2001). Rethinking Family Structure and Single Parenthood: Implications for Future. *The well-being of children and families: Research and data needs*, 127.

Butler, R., & Butler, M. (2015). The password practices applied by South African online consumers : perception versus reality : original research. *South African Journal of Information Management, 17*(1), 1-11. doi:doi:10.4102/sajim.v17i1.638

Calvete, E., Orue, I., Estévez, A., Villardón, L., & Padilla, P. (2010). Cyberbullying in adolescents: Modalities and aggressors' profile. *Computers in Human Behavior, 26*(5), 1128-1135. doi:https://doi.org/10.1016/j.chb.2010.03.017

Campbell, D. T., & Stanley, J. C. (2015). *Experimental and quasi-experimental designs for research*: Ravenio books.

Chadwick, R., & Knight, P. (2012). Cybersmart: Learning online safety. *TEACH Journal of Christian Education, 4*(2), 8.

Chipangura, B., & Dtendjo-Ndjindja, G. (2022). Securing the cybersafety of South African online high school learners beyond COVID-19. *The Journal for Transdisciplinary Research in Southern Africa, 18*(1), 8.

Cilliers, L., & Chinyamurindi, W. (2020). Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa. *The Electronic Journal of Information Systems in Developing Countries, 86*(4), e12131.

Daud, A., Omar, S. Z., Hassan, M. S., Bolong, J., & Teimouri, M. (2014). Parental mediation of children's positive use of the Internet. *Life Science Journal, 11*(8), 360-369.

David, S., Hana, Machackova, Giovanna, M., Lenka, D., Elisabeth, S., . . . Uwe, H. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. doi:10.21953/lse.47fdeqj01ofo

Dunn-Coetzee, M. (2015). A psycho-educational strategy as tool for educating adolescents on internet safety. *The Social Work Practitioner-Researcher, 27*(3), 306-321.

Etikan, I., & Bala, K. (2017). Sampling and sampling methods. *Biometrics & Biostatistics International Journal, 5*(6), 00149.

Feinberg, T., & Robey, N. (2009). Cyberbullying. *The education digest, 74*(7), 26.

Fund, U. N. C. (2019). Growing up in a connected world. Retrieved from https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8*(4), 597-607.

James, P. A., & Kur, J. T. (2020). Parental Mediation of Childrens Risky Experiences with Digital Media. *The Journal of Society and Media, 4*(2), 298-318.

John W., C. (2009). *Third Edition Research Design: Qualitative, Quantitative and Mixed Methods Approaches*: Sage Publications, Inc.

Johnson, B., & Ray, W. (2016). Family Systems Theory. In.

Kesavelu, D., Sheela, K., & Abraham, P. (2021). Stages of Psychological Development of Child-An Overview. *Int J Cur Res Rev| Vol, 13*(13), 74.

KOCOGLU, E. (2021). Individual Seeking Identity in the Digital World. *The Eurasia Proceedings of Educational and Social Sciences, 20*, 20-23.

Kortjan, N., & Von Solms, R. (2013). *A cyber security awareness and education framework for South Africa.* Nelson Mandela Metropolitan University,

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal, 52*(1), 29-41.

Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African computer journal = Suid-Afrikaanse rekenaartydskrif, 29*(2), 16-35. doi:10.18489/sacj.v29i2.471

Lange, M. d. (2012). Guidelines to Establish an e-Safety Awareness in South Africa.

Lee, C., & Shin, N. (2017). Prevalence of cyberbullying and predictors of cyberbullying perpetration among Korean adolescents. *Computers in Human Behavior, 68*, 352-358. doi:https://doi.org/10.1016/j.chb.2016.11.047

Lee, S.-J. (2013). Parental restrictive mediation of children's internet use: Effective for what and for whom? *New media & society, 15*(4), 466-481.

Lester, T. M. (2018). *An Investigation on Cyber Safety Awareness Among Teachers and Parents.* (Ed.D.). Gardner-Webb University, Ann Arbor. Retrieved from https://www.proquest.com/dissertations-theses/investigation-on-cyber-safety-awareness-among/docview/2247902471/se-2?accountid=15083 ProQuest Central; ProQuest Dissertations & Theses Global database. (10845057)

*Livingstone, S., Lse, Davidson, J., Bryce, J., With, S., Batool, C., Haughton, A. and Nandi (2017). Children's online activities, risks and safety A literature review by the UKCCIS Evidence Group. [online] Available at: https://www.lse.ac.uk/business/consulting/assets/documents/childrens-online-activities-risks-and-safety.pdf.*

Ljubojev, N., Glusac, D., & Radosav, D. (2017). CHILDREN IN THE INTERNET: PROTECTION AND PARENTS'PERCEPTION. *Chapter, 9*, 105-120.

Marais, J. (2012). *A framework for parental control of mobile devices in South Africa.* Nelson Mandela Metropolitan University,

NIST (2012). Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1 JOINT TASK FORCE TRANSFORMATION INITIATIVE. [online] Available at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf.

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. *Predicting and changing health behaviour: Research and practice with social cognition models, 3*, 70-106.

Nurse, J. R. (2021). Cybersecurity awareness. *arXiv preprint arXiv:2103.00474*.

Ofcom. (2020). Internet users' experience of potential online harms: summary of survey research. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0024/196413/concerns-and-experiences-online-harms-2020-chart-pack.pdf

Ong, M. H. A., & Puteh, F. (2017). Quantitative data analysis: Choosing between SPSS, PLS, and AMOS in social science research. *International Interdisciplinary Journal of Scientific Research, 3*(1), 14-25.

Paraiso, E. L. (2019). *Towards a cyber safety information framework for South African parents.* University of Pretoria,

Pfeiffer, S., & In-Albon, T. (2022). 1.10 - Family Systems. In G. J. G. Asmundson (Ed.), *Comprehensive Clinical Psychology (Second Edition)* (pp. 185-201). Oxford: Elsevier.

Prior, S., & Renaud, K. (2020). Age-appropriate password "best practice" ontologies for early educators and parents. *International Journal of Child-Computer Interaction, 23*, 100169.

Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-85.

Rani, A., & Shreshtha, M. (2021). Adoption of Parental Mediation Strategies for Teenagers' Internet Use. *Elementary Education Online, 20*(5), 4964-4964.

Renaud, K., & Prior, S. (2021). The “three M’s” counter-measures to children’s risky online behaviors: mentor, mitigate and monitor. *Information & Computer Security, 29*(3), 526-557.

Shrestha, N. (2021). Factor analysis as a tool for survey analysis. *American Journal of Applied Mathematics and Statistics, 9*(1), 4-11.

Singh, A. M. (2008). Parental protection of children online : peer reviewed article. *South African Journal of Information Management, 10*(2), 1-13. doi:doi:10.10520/AJA1560683X_250

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian journal of psychology, 49*(2), 147-154.

Toit, R. D., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity : a South African context. *Acta Criminologica : African Journal of Criminology & Victimology, 31*(3), 111-131. doi:doi:10.10520/EJC-14d9e12e41

UK. (2016). *NATIONAL CYBER SECURITY STRATEGY 2016-2021*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

UNICEF. (2019). *Adolescent development and participation*. Retrieved from https://www.unicef.org/adolescence

Walrave, M., & Heirman, W. (2011). Cyberbullying: Predicting victimisation and perpetration. *Children & Society, 25*(1), 59-72.

Willard, N. E. (2007). *Cyber-safe kids, cyber-savvy teens: Helping young people learn to use the Internet safely and responsibly*: John Wiley & Sons.

Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). *Parents just don't understand: Why teens don't talk to parents about their online risk experiences.* Paper presented at the Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing.

Wisniewski, P., Xu, H., Rosson, M. B., Perkins, D. F., & Carroll, J. M. (2016). *Dear diary: Teens reflect on their weekly online risk experiences.* Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.

Zaman, B., & Nouwen, M. (2016). Parental controls: advice for parents, researchers and industry. *EU Kids Online*.

# APPENDIX A

**Permission Request Letter for the School**


University of the Witwatersrand,

Faculty of Commerce, Law and Management

[Contact person]

[Organisation name]

[Organisation address]

[Date]

Dear Sir/Madam,

Re: Permission to conduct research at Pretoria East Reddford House The Hills

My name is Hangwelani Masutha.

I am a Master of Management student in the field of Digital Business at the University of the Witwatersrand. I am seeking permission to do research at Reddford House, The Hills.

I am conducting research on cybersecurity, investigating the level of parents' awareness on the risks which impact children in the context of South Africa.

Recent studies reported an increase in cases and incidents where children get exposed to inappropriate content at very early stages, cyberbullying, inappropriate online friendships which put them at risk of paedophiles etc. thus affecting their wellbeing and development.

My main focus is on parents with children between the of 3 and 12 years as research has noted this age bracket as the most vulnerable. The emphases Is on increasing awareness in our society and highlighting the need for parents to ensure safety for their children as they access the internet and all the digital platforms.

As one of the parents in your school I have chosen your school as it perfectly fits the profile of participants required for this study. I also believe that the topic around cybersecurity risks and its impact on children is one that we as communities and societies need to consciously and continuously increase awareness to, in order to build a healthy next generation.

The research will entail collecting data from the parents and will request demographic information including their age, gender, education and employment status. The survey will remain anonymous and will not request any of their direct personal information such as name, surname, residential address etc.

I request permission that you distribute my online survey questionnaire to the parents in the school through your email distribution system and if possible, through the Reddford application tool which you normally send communication and notifications to parents.

I will invite parents from your school to participate in this survey study. If they agree, they will be asked to answer the questionnaire. The participants will be required to set aside approximately 5 to 10 minutes to complete the survey. They can complete the survey any time of the day as the link will be available 24x7 for the duration of the study between September 2022 and January 2023.

A participation letter will be shared informing the participants of the research background, amount of time it will approximately take them and informing them of the anonymity and confidentiality of their submission. Individual privacy will be maintained in all published and written data resulting from the study.

The results will be communicated to the University of the Witwatersrand as part of the dissertation.

The research participants will not be advantaged or disadvantaged in any way. They will be reassured that they can withdraw their permission at any time during this project without any penalty. There are no foreseeable risks in participating in this study. The participants will not be paid for this study.

All research data will be preserved anonymously for reuse by other researchers.

I therefore request permission in writing to conduct my research at your organization. The permission letter should be on your organization's headed paper, signed and dated, and specifically referring to myself by name and the title of my study.

Please let me know if you require any further information. I look forward to your response as soon as is convenient.

Yours sincerely,

Hangwelai Masutha

Contact: 0829304730

Email: 1884336.students@wits.co.za

Dr Kiru Pillay

Wits contact number

Wits email address]

# APPENDIX B

**Permission Request Letter for the church**

University of the Witwatersrand,

Faculty of Commerce, Law and Management

[Contact person]

[Organisation name]

[Organisation address]

[Date]

Dear Sir/Madam,

Re: Permission to conduct research at Calvary Christian Church Pretoria

My name is Hangwelani Masutha.

I am a Master of Management student in the field of Digital Business at the University of the Witwatersrand. I am seeking permission to do research at Calvary Christian church PE.

I am conducting research on cybersecurity, investigating the level of parents' awareness on the risks which impact children in the context of South Africa.

Recent studies reported an increase in cases and incidents where children get exposed to inappropriate content at early stages, cyberbullying, inappropriate online friendships which put them at risk of paedophiles etc. thus affecting their wellbeing and development.

The main focus is on parents with children between the age of 3 and 12 years as research has noted this age bracket as the most vulnerable. The emphases Is on increasing awareness in our society and highlighting the need for parents to ensure safety for their children as they access the internet and all the digital platforms.

The church perfectly fits the profile of the participants required for this study due to the understanding that this is a family church and has families with children.

The research will entail collecting data from the parents and will request demographic information including their age, gender, education, and employment status. The survey will remain anonymous and will not request any of their direct personal information such as name, surname, residential address etc.

I request permission that you distribute the online survey questionnaire to the parents in the church through your email distribution system. Should the participants agree to form part of the survey, they will be asked to answer the questionnaire. The participants will be required to set aside approximately 5 to 10 minutes to complete the survey. They can complete the survey any time of the day as the link will be available 24x7 for the duration of the study between September 2022 and January 2023.

A participation letter will be shared informing the participants of the research background, amount of time it will approximately take them and informing them of the anonymity and confidentiality of their submission. Individual privacy will be maintained in all published and written data resulting from the study.

The results will be communicated to the University of the Witwatersrand as part of the dissertation.

The participants will not be advantaged or disadvantaged in any way. They will be reassured that they can withdraw their permission at any time during this project without any penalty. There are no foreseeable risks in participating in this study. The participants will not be paid for this study.

All research data will be preserved anonymously for reuse by other researchers.

I therefore request permission in writing to conduct my research at your organization. The permission letter should be on your organization's headed paper, signed and dated, and specifically referring to myself by name and the title of my study.

Please let me know if you require any further information. I look forward to your response as soon as is convenient.

Yours sincerely,

Hangwelai Masutha

Contact: 0829304730

Email: 1884336.students@wits.co.za

Dr Kiru Pillay

Wits contact number

Wits email address

# APPENDIX C

## Participant Information Sheet (PIS)

Dear Sir / Madam

My name is Hangwelani Masutha. I am a Master of Management student in the field of Digital Business at the University of the Witwatersrand. I am conducting a research study about cybersecurity risks titled, "Investigating levels of cybersecurity risks awareness by South African parents" under the supervision of Dr Kiru Pillay.

The study focuses on parents with children between the age of 4 and 12 years, as research has noted this age bracket being the most vulnerable. The emphases are on increasing awareness in our society and highlighting the need for parents to ensure safety for their children as they access the internet and all the digital platforms.

Considering the study, I would like to invite you to take part in my research and answer an online survey questionnaire.

Should you decide to take part, your participation in this survey will take you approximately 5-10 minutes to complete and you can access it any time of the day. The survey is completely voluntary and will remain anonymous and confidential. The survey will not collect any personal identification information such as name, surname, residential address etc, but only demographic information which include your age, gender, education, and employment status.

The research will not be advantageous or disadvantageous to you in any way. You may also withdraw permission to complete the survey at any time without any penalty. There are no foreseeable risks in participating in this study and you will not be paid for this study.

On completion of this research study, it will be written up as a research report. The report will be available on the university library website.

If you have any questions during or afterwards about this research study, feel free to contact me or my supervisor on the details listed below. If you have any concerns or complaints about the ethical procedures of this research study, you are welcome to contact

the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

Yours sincerely,

Hangwelani Masutha

Researcher:

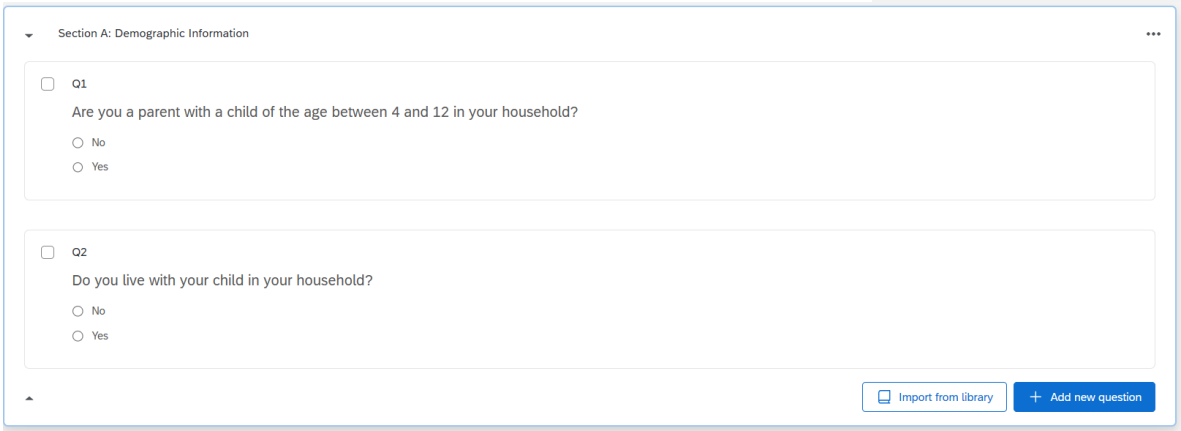
Hangwelani Masutha, Wits email, 1884336.students@wits.ac.za

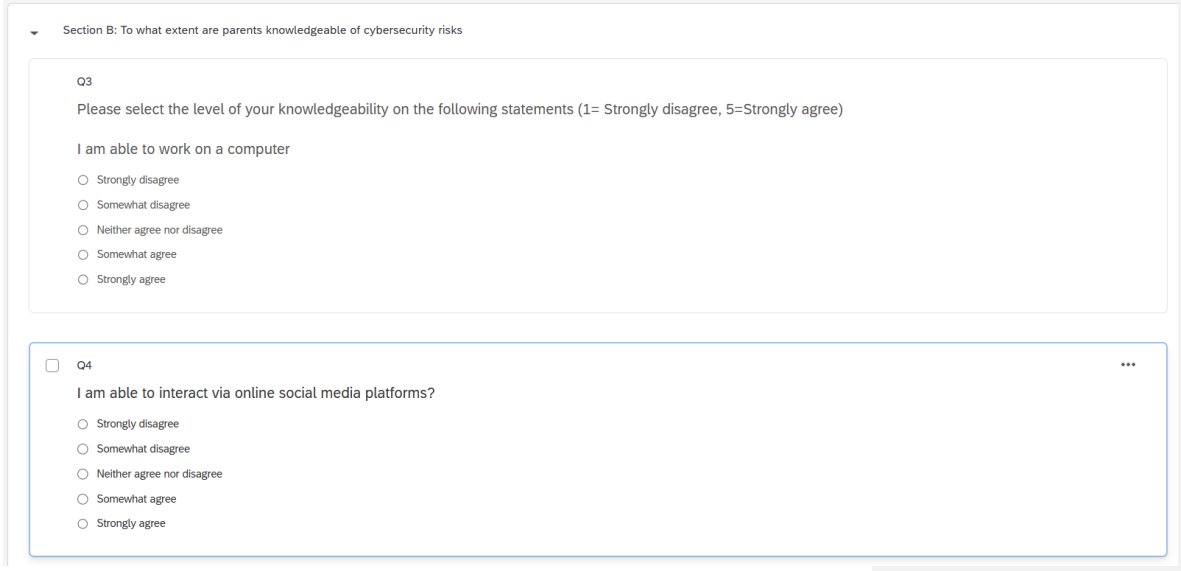
Supervisor:

Dr Kiru Pillay, Wits email, Wits phone number

# APPENDIX D

## Survey Questions



Q5

I am aware and knowlegeable on these cybersecurity risks

| | Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree |
|---|---|---|---|---|---|
| Cyberbullying | ○ | ○ | ○ | ○ | ○ |
| Cyberstalking | ○ | ○ | ○ | ○ | ○ |
| Stranger danger | ○ | ○ | ○ | ○ | ○ |
| Identify scam | ○ | ○ | ○ | ○ | ○ |
| Phishing scam | ○ | ○ | ○ | ○ | ○ |

Q6

I am aware and knowledgeable of the potential risks faced while interacting on the following internet services

| | Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree |
|---|---|---|---|---|---|
| Online Gaming | ○ | ○ | ○ | ○ | ○ |
| Chat groups | ○ | ○ | ○ | ○ | ○ |
| Instagram, facebook,tik tok, twitter etc | ○ | ○ | ○ | ○ | ○ |
| ecommerce platform | ○ | ○ | ○ | ○ | ○ |

Section C: To what extent are parents educating children on safety practices

Q7

Please select the extent to which you disagree or agree with the following statements (where 5=strongly agree)

I actively talk to my child about internet use

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Q8

I teach my child to keep personal information private (e.g not share phone numbers, adresses, credit card info etc)

- ○ Strongly disagree
- ○ Somewhat disagree
- ○ Neither agree nor disagree
- ○ Somewhat agree
- ○ Strongly agree

Q9

I encourage my child to come to me if they encounter a problem while online (e.g. being bullyied, getting directed to inappropriate sites etc)

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Section D: To what extent are parents implementing proactive security measures

Q10

Please select the extent to which you disagree or agree with the following statements (1=strongly disagree, 5=strongly agree)

I am aware of the following tools or technologies that can assist in keeping my child safe while online?

| | Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree |
|---|---|---|---|---|---|
| Firewall | ○ | ○ | ○ | ○ | ○ |
| Spam blocker | ○ | ○ | ○ | ○ | ○ |
| Filtering software | ○ | ○ | ○ | ○ | ○ |
| Time limiting software | ○ | ○ | ○ | ○ | ○ |
| Monitoring Software | ○ | ○ | ○ | ○ | ○ |
| Online purchase payment passwords | ○ | ○ | ○ | ○ | ○ |

Q11

I have applied practical measures to protect my child while online (e.g. change passwords, apply browser filters, anti-virus, spam blocker etc)?

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Q12

I actively monitor my childs online activity (e.g. Check browser history,Check online account,Messages,Contacts)

- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

# APPENDIX E

Survey- Output 2.xlsx

Field Code Changed