Online Risk Awareness and Safety Needs of Children: A Zimbabwean Perspective

Gift Kalisto Machengete[1], Maxwell Sandada[2], Cryford Mhaka[3], Felicity Kaseke[4]

Abstract: Given growing concerns about exposure to online risks, this study investigates children's risk awareness and online safety needs in Zimbabwe. The research focuses on assessing factors influencing children's awareness of online dangers and examining how demographic factors impact the perceived need for online safety education. While prior studies emphasise, the tangible risks posed by online interactions and the role of digital literacy, limited research has addressed these challenges within Zimbabwe's context. This study builds on existing research to bridge the gap by providing localized insights. Data was collected through structured questionnaires administered to 2,617 children aged 8 to 18 across Zimbabwe's ten provinces. Analytical methods included chi-square tests, logit regression and analysis of variance. Key findings indicate that older children and frequent Internet users are more aware of online risks. They also highlighted that meeting online friends in person significantly increases their exposure to harm. These findings provide valuable insights for policymakers, educators, and

[1] Director General, Postal & Telecommunications Regulatory Authority of Zimbabwe, Harare, Zimbabwe, Address: 1110 Performance Close Mt Pleasant Business Park, Harare, Zimbabwe, Corresponding author: machengete@potraz.zw.

[2] Research and Development Unit, Postal & Telecommunications Regulatory Authority of Zimbabwe, Harare, Zimbabwe, Address: 1110 Performance Close Mt Pleasant Business Park, Harare, Zimbabwe, E-mail: sandada@potraz.zw.

[3] Research and Development Unit, Postal & Telecommunications Regulatory Authority of Zimbabwe, Harare, Zimbabwe, Address: 1110 Performance Close Mt Pleasant Business Park, Harare, Zimbabwe, E-mail: mhaka@potraz.zw.

[4] Research and Development Unit, Postal & Telecommunications Regulatory Authority of Zimbabwe, Harare, Zimbabwe, Address: 1110 Performance Close Mt Pleasant Business Park, Harare, Zimbabwe, E-mail: kaseke@potraz.zw.

parents to craft effective interventions, including targeted safety education and enhanced regulatory frameworks for safer online environments. This study contributes to understanding online risk awareness and safety needs among Zimbabwean children.

Keywords: Digital Literacy; Online Safety; Child Internet Use; Cybersecurity Awareness; Risk Management

1. Introduction

The widespread use of Information and Communication Technology (ICT) offers considerable opportunities to society, and both adults and children are using the Internet to meet some of their educational and entertainment needs (Dzoro et al., 2019; Moyo et al., 2022; Tsokota et al., 2022). Internet-related attacks have become prevalent and are expected to increase as reliance on the Internet increases (Mutunhu et al., 2022). Many schools in Zimbabwe now allow learners to access the Internet and share educational material through ICT devices (Moyo et al., 2022). The Zimbabwe education system has adopted the use of ICT devices popularly known as digitalised learning (Dzingirayi & Musemburi, 2023). However, the Internet contains information that has adverse impacts on the psychosocial and sexual development of children. Furthermore, children are not sufficiently equipped to navigate cyber-related risks (Dzoro et al., 2019; Moyo, et al., 2022). Most Zimbabwean students who are not adequately prepared for e-safety are now entering universities and are thus exposed to the risks posed by ICT (Tsokota et al., 2022). Learners using ICTs face Internet and social media-related risks which expose them to inappropriate content, communicating and meeting strangers, cyberbullying, ICT addiction and cyber-harassment (Moyo et al., 2022). The social media syndrome is a technological fashion that has defeated the expected ubuntu/hunhu behaviour and has immensely contributed to cyberbullying amongst learners (Mabvurira et al., 2022; Dzingirayi & Musemburi, 2023). Mutunhu et al. (2022) highlighted that students and staff at Zimbabwe’s universities need to have the requisite knowledge and understanding of the importance of cybersecurity principles and be made aware of how to protect their data. Cyber security has become essential in everyday life; therefore, cyber security awareness is critical in protecting people and systems against cyber threats (Mutunhu et al., 2022). Sadly, most parents, teachers and learners do not have the knowledge and expertise to mitigate these ICT risks (Moyo et al., 2022).

Despite these growing concerns, there is limited research on factors influencing risk awareness among Zimbabwean children and their specific needs for online safety measures. This study aimed to fill this gap by investigating the current state of risk awareness among children in Zimbabwe and identifying their online safety needs. The findings inform policymakers, educators, and parents about the necessary steps to protect children in the digital age, ensuring they can safely benefit from the Internet's opportunities.

1.1. Statement of Problem

Opportunities and dangers exist as the Internet becomes increasingly available and utilised among Zimbabwe's youth. According to the Global Kids Online Zimbabwe report, a considerable 70% of children between the ages of 9 and 17 have access to the internet either for educational purposes or social connectivity (Global Kids Online, 2020). Nearly 35% of children aged 10 to 18 have experienced some form of online harassment (UNICEF, 2021), and this may be attributed to the fact that children in developing countries (Zimbabwe included) are often not equipped to navigate online environments leading to increased vulnerability to exploitation and abuse (Internet Society, 2022). The Child Rights International Network (2019) report emphasised how many parents and guardians did not understand children's specific online needs, which impaired their ability to develop protective strategies.

1.2. Objectives of the Study

The specific objectives of the research were as follows:

1) To assess the factors influencing children's awareness of online risks in Zimbabwe.
2) To examine the impact of demographic factors on the perceived need for online safety education among children in Zimbabwe.
3) To explore the association between children's online activities and their exposure to online risks in Zimbabwe.

1.3. Significance of the Study

Children in Zimbabwe increasingly use online platforms for education, entertainment, and social interaction; hence, it is critical to understand the key factors that shape their awareness of online dangers. By identifying these factors and understanding demographic variations, the study helps policymakers, educators, and regulatory bodies to develop targeted educational programs, awareness campaigns, and policy interventions tailored to improve digital literacy and safety practices among Zimbabwean children. The study also helps identify specific activities that most increase children's vulnerability to online dangers. This local study helps to ensure that interventions are contextually relevant and raises public awareness about the importance of online safety for children, encouraging a broader conversation among stakeholders, including the government, the private sector, civil society, and the public. This research also serves as a benchmark for future research on online safety in Zimbabwe, allowing for comparisons over time and assessing the effectiveness of initiatives put in place.

2. Literature Review

2.1. Introduction

The Internet enhances comfort and convenience by enabling online work, study, and entertainment, potentially improving children's social well-being (Yuliana., 2022). In the age of digital transformation, children are often exposed to psychological damage, abuse, and violence owing to a lack of Internet monitoring (Yujin et al., 2023; Yuliana, 2022). Online safety is often used interchangeably with Internet safety, cyber safety, Internet security, online security, and cyber security (Yujin et al., 2023). While online safety is crucial for protecting children from harmful content, it is important for parents not to discourage digital technology use, as it can significantly enhance their lives by providing valuable entertainment, information, and learning opportunities (Yujin et al., 2023; Allison, 2018; Green et al., 2019). Multiple research studies have identified that girls and young women face a greater risk of harm online. 86% of images of child sexual exploitation and abuse identified by IWF in 2017 were of girls, and 59% of girls/young women aged 11-21 say social media is a significant cause of stress (Green et al., 2019).

2.2. Children’s Use of the Internet

According to Allison (2018), mobile technologies like smartphones have reshaped adolescent communication, intertwining it with various risks, many of which are sexual in nature. Children today spend significant time online for education and entertainment, including accessing learning platforms, watching videos, playing games, and using social media (Yujin et al., 2023). The Internet also serves as a hub for social interaction, allowing children to connect with friends and family through messaging apps and social networks (Yuliana, 2022; Hawkins, 2017). Social media platforms like Facebook, Instagram, and WhatsApp are popular among children for communication and social interaction, though age restrictions are often ignored. Children also use the Internet for games, videos, and other interactive content. Platforms like YouTube, TikTok, and online gaming communities draw significant engagement from children, contributing to their digital literacy (Mabvurira et al., 2022). However, children’s lack of critical judgment makes them vulnerable to online risks like cyberbullying, harmful content, and misleading commercial practices (Yujin et al., 2023). Research shows that parents with higher socioeconomic status are more likely to offer online support and actively monitor their children’s screen time, significantly influencing how children use the Internet (Green et al., 2019; Hawkins, 2017). Children’s online experiences are shaped by various risk factors related to their emotional, cognitive, and social development. However, pinpointing the exact moment they encounter specific online risks is often complicated and usually only precise in hindsight (Davison et al., 2017). The motives for cyberbullying among high school learners include differences, peer pressure, exposure to violent media, intimate relationships, fun and boredom, low self-esteem and jealousy (Mabvurira et al., 2022).

2.3. Online Risks

Online safety risks for children and youth include cyberbullying, stalking, image-based abuse, exposure to harmful content like pornography, and privacy breaches while using electronic devices to access the Internet and social media (Yujin et al., 2023; Yuliana, 2022; Mabvurira et al., 2022). These risks can result in emotional, psychological, financial, or physical harm, often stemming from the misuse of personal data, misinformation, and unsafe commercial practices (Yujin et al., 2023; Allison, 2018; Chingoriwo, 2022; Moyo et al., 2022). Online safety, including child online safety, particularly cybersecurity, is widely acknowledged as a national priority in many nations across the globe (Muhingi et al., 2020). According to Green et al. (2019), online risks emerge from multiple factors, including complex interactions between individual capabilities, home, school and peer group contexts and the opportunities of online environments. The misuse of advanced digital technologies and inadequate parental supervision further endanger their privacy, financial security, and legal rights (Yujin et al., 2023; Muhingi et al., 2020). Children facing family difficulties are especially vulnerable online, with factors like socioeconomic status, educational transitions, gender, sexuality, family support, and special educational needs further increasing their risk of online harm (Green et al., 2019). People who can handle some online adversity may develop digital resilience, but those who are already at risk offline are more likely to face heightened vulnerability online (Davison et al., 2017).

2.4. Children's Awareness of Online Risk

Online risk awareness refers to the understanding and knowledge of potential dangers and threats that individuals may encounter while using the Internet (Muhingi et al., 2020). Due to their age, children struggle to evaluate the risks and benefits of using the Internet, often unaware of potential dangers until it is too late, making them vulnerable to online abuses and long-term privacy issues (Dzoro et al., 2019; Allison, 2018; Lee et al., 2014). Children often do not fully understand the consequences of sharing personal information, sending images or arranging to meet strangers online (Green et al., 2019). Age is the key factor differentiating children's online experiences, and gender is also significant (Davison et al., 2017). A lack of awareness among adults and children about the dangers of electronic media hinders adequate online safety precautions, making awareness campaigns and safety programs essential for protecting children (Muhingi et al., 2020). The widespread exposure to online pornography among teenagers highlights the need for comprehensive sex education to address potential adverse effects (Davison et al., 2017). Online risk awareness is crucial for enabling safe and responsible Internet use, especially for vulnerable groups like children.

2.5. Online Safety Needs

A lack of awareness among both adults and children about the dangers of electronic media hinders adequate online safety precautions, making awareness campaigns and safety programs essential for protecting children (Muhingi et al., 2020; Farzana et al., 2021; Hawkins, 2017). Mobile technologies are integral to early adolescent social interactions, but parental awareness is crucial for managing risks such as exposure to pornography and contact with strangers (Allison, 2018). Children with uninformed or less confident parents are more vulnerable to online risks, particularly if they face other life challenges. This highlights the need to support parents, careers, and teachers in developing authoritative parenting skills for managing children's digital lives (Allison, 2018; Green et al., 2019). Children should be educated in digital literacy and cybersecurity to avoid risky online behaviours, protect their privacy, and stay safe from threats like phishing, pornography, cyberbullying, and identity theft (Yuliana, 2022). To minimize significant online risks for children and youth in cyberspace, it is necessary to maintain a regulatory approach to the online exposure of children under the age of 13 (Yujin et al., 2023). In summary, online safety needs for children encompass education and awareness, parental supervision, digital literacy, safe online spaces, and legal and policy protections. Learners' online activities must be monitored at home and school to create a cyber-bullying-free learning environment. (Mabvurira et al., 2022). School-based counselling is a noble practical guide that shapes and corrects the behaviour of learners (Dzingirayi & Musemburi, 2023). To make children's online presence safer, Dzoro et al. (2019) recommended the active and informed involvement of parents and deliberate state-supported, stakeholder-driven programmes that recognise the agency of educating children on cyber ethics and relevant legal protections.

There is a need for stronger physical security of ICT assets and cybersecurity legislation (Chingoriwo, 2022). Mutunhu et al. (2022) highlighted that universities should implement comprehensive awareness and education programs for the adoption of necessary safety measures. Mabvurira et al. (2022) added that there is a need for high school learners to be educated on safe and healthy methods of using information communication technologies. There is a need to devise a deliberate training programme that has its bedrock on Afrocentric culture and to ensure that all school counsellors receive adequate contemporary skills. (Dzingirayi & Musemburi, 2023)

2.6. Analysis and Policy Implications

The aim of creating awareness is to educate technology users on the potential risks faced when using Internet communication tools, such as social media, chat rooms, online gaming, email, and instant messaging on various devices, including smartphones. Online safety issues related to digital device use, such as media addiction, should be addressed from the perspective of the entire domestic and global system surrounding children and youth (Yujin et al., 2023). It requires a global, multi-level policy approach involving international cooperation and national agencies for children's online safety, while locally, parents and teachers should work together to provide digital literacy education and guidance (Yujin et al., 2023). Adults should develop and implement policies that enhance children's online experiences, using a comprehensive approach that includes national and international cooperation with states, organizations, and digital firms to create effective laws and guidelines for children's well-being. Future research should focus on creating parental education programs and screening tools for nurses to manage mobile technology use and its risks better. It should also develop practical tools to assess online risks and improve the technology skills of both nurses and parents (Allison, 2018).

Numerous programs have been introduced globally, and interventions have been proven to help improve children's online safety. For example, the "Be Internet Awesome" initiative presented by Google teaches children how to face several dangers posed to them online, like fishing and online bullying (Google, 2018). Likewise, in Australia, the e-Safety Commissioner has been able to coordinate resources and training for parents and educators as one strategy for digital safety (Australian Government e-Safety Commissioner, 2022). These cases indicate that a combination of interventions, including education, parental involvement, and public policy, can enhance children's Internet safety.

When considering the different contexts within which children's online experiences can be understood, they must be understood within the vectors of personal risks associated with different populations. National Center for Missing & Exploited Children (2018), in some cases, notes that subpopulations are distinct; for example, they point out that LGBTQ youth suffer more Internet abuse than other groups. By considering a wider demographic context, policies could formulate specific interventions necessary for each sub-group of children, including those who are often the most at risk within these digital contexts.

3. Methodology

3.1. Research Design

This methodology aims to comprehensively understand risk awareness and the online safety needs of children in Zimbabwe. The researchers used a quantitative approach to investigate the children’s online risk awareness and safety needs. The survey targeted children aged 8 to 18 across all of Zimbabwe’s ten (10) provinces, including urban and rural areas. Structured interviews were used to collect data from the children. In this study, the researchers were interested in larger-scale data collection to understand what factors influence children’s online risk awareness, examine the impact of demographic factors on the perceived need for online safety education and explore the association between children’s online activities and their exposure to online risks.

3.2. Sampling

The survey had a sample size of 2,617 children, of which 55% were girls and 45% were boys. Respondents were selected using a four-stage multiple-sampling technique for the interviews to ensure representation across different demographic segments. Schools were initially grouped or stratified by provinces. Within each province, schools were further stratified based on Capitation Grant Classifications (CGC). The CGC is a criterion used by the Ministry of Primary and Secondary Education to categorise schools in terms of resources and location. Schools were selected randomly from each province, and purposive sampling was used to choose children within each school for interviews.

3.3. Data Collection

Data collection was done through structured questionnaires administered to the children in schools. The questionnaires covered demographic information (age, gender, province, school attended, education level), frequency of Internet usage, types of online activities, awareness of online risks (cyberbullying, privacy invasion, exposure to inappropriate content), and the perceived need for online safety education. Parental supervision was also addressed through questions aimed at understanding the extent of their involvement in children’s online activities.

3.4. Data Analysis

The data analysis was done using Python, leveraging its robust statistical and data analysis libraries to perform the Logit regression analysis, ANOVA and Chi-square tests. The Logit Regression analysis assessed the factors influencing children's awareness of online risks. The dependent variable was children's awareness (binary outcome: aware vs. unaware), while predictor variables: age, gender, education level, school attended, province, access to devices, parental guidance, and frequency of Internet usage were incorporated into the model. ANOVA was employed to examine the impact of demographic factors on the perceived need for online safety education. The mean differences between age groups, gender, education level, province and school attended were compared based on the collected responses. The Chi-Square tests were carried out to explore the association between children's online activities and their exposure to online risks. The tests helped determine whether there were statistically significant relationships between different online activities and encountering online risks.

3.5. Validity

To ensure content validity, the study was conducted in collaboration with experts in child psychology from the Ministry of Primary and Secondary Education. A pilot study was conducted with a small group of participants to test the instrument's reliability, and necessary adjustments were made based on feedback.

3.6. Ethical Considerations

Given the sensitive nature of the research involving children, ethical approval was sought from the Ministry of Primary and Secondary Education. Informed consent was obtained from teachers, and agreement was obtained from the children participating in the study. The privacy and confidentiality of the respondents were maintained throughout the research. The data collected was anonymised to protect the children's identity, and their participation was voluntary, with the option to withdraw at any point. To ensure reliability, a threshold of Cronbach's Alpha coefficient of 0.7 was used.

4. Findings

4.1. Reliability

The study yielded a Cronbach’s Alpha of 0.8114, indicating high internal consistency. Cronbach’s Alpha indicates solid internal consistency among survey items, which confirms that the scale is reliable in measuring children’s awareness of online risks in Zimbabwe.

Table 1. Multicollinearity check using Variance Inflation Factor (VIF)

Variable	VIF
Gender	0.399777
Age	2.88017
Education level	1.2551
School attended	2.643952
Province	3.540047
Access to Devices	1.47684
Frequency of Internet Usage	4.04564
Awareness of the risks	2.12707
Aware of online safety practices	1.56337
Guidance on Internet	1.10235

The VIF values in Table 1 above indicate that multicollinearity is not an essential issue in the model. Most variables have VIF values well below the standard threshold of 5, which shows that the predictors are generally independent, ensuring the regression coefficients’ stability and reliability.

4.2. Factors Influencing Children’s Awareness of Online Risks in Zimbabwe

The logit regression analysis was employed to assess the factors influencing children’s awareness of online risks in Zimbabwe, shown in the tables below.

Table 1. Logit Regression Results

Dependent Variable:	**Awareness of the Risks**	**No. Observations:**	**2617**
Model:	Logit	**Df Residuals:**	2606
Method:	MLE	**Df Model:**	10
Pseudo R-squared:	0.54580	**Log-Likelihood:**	-1515.8
Converged:	True	**LL-Null:**	-1676.4

Dependent Variable:	**Awareness of the Risks**	**No. Observations:**	**2617**
Covariance Type:	Nonrobust	**LLR p-value:**	5.104e-63

The results in Table 2 indicate that the model effectively explains children's awareness of online risks in Zimbabwe, considering a Pseudo R-squared value of 0.54580. The model is statistically significant, as shown by the very low LLR p-value of 5.104e-63, and the substantial improvement in Log-Likelihood from -1676.4 in the null model to -1515.8 confirms that the predictors meaningfully contribute to explaining awareness of online risks. The successful convergence of the model further assures the reliability of these results. These findings imply that the examined factors are highly influential in shaping children's awareness of online risks in Zimbabwe.

Table 2. Logit Regression Model Results

	coef	**std err z**	**P>|z|**	**[0.025**	**0.975]**
const	-2.1604	0.391-5.519	0.000	-2.928	-1.393
Gender	-5.1545	0.089-1.740	0.082	-5.329	0.020
Age	2.4482	0.0885.117	0.000	2.277	2.620
Education level	6.0103	0.0033.247	0.001	6.004	6.016
School attend	-2.0033	0.002-1.342	0.180	-0.008	2.002
Province	1.0185	0.0161.145	0.252	-0.013	1.050
Access to Devices	5.1409	0.0542.623	0.009	5.036	5.246
Frequency of Internet Usage	3.0240	0.0121.980	0.048	0.000	3.048
Aware of online safety practices	5.1386	0.09611.815	0.000	0.950	1.327
Guidance on Internet	1.6473	0.0966.750	0.000	1.459	1.835

The logit regression results in Table 3 above give meaningful insights into the determinants of children's online risk awareness in Zimbabwe. The results show that **age** (coef = 2.4482, p < 0.001) is a highly significant factor, suggesting that as children grow older, their awareness of online risks increases. Similarly, **education level** (coef = 6.0103, p = 0.001) has a significant and positive coefficient, highlighting that higher education significantly enhances children's awareness of online risks, possibly due to more comprehensive education on Internet safety. **Access to devices** (coef = 5.1409, p = 0.009) shows a strong positive relationship with children's awareness of online risks; this means having access to devices increases children's awareness of online risks due to greater exposure to the Internet.

The **frequency of Internet usage** (coef = 3.0240, p = 0.048) is slightly significant, showing that more frequent Internet usage, to some extent, increases awareness of online risks.

Furthermore, **awareness of online safety practices** (coef = 5.1386, p < 0.001) and **guidance on Internet usage** (coef = 1.6473, p < 0.001) are both very significant, highlighting the importance of proactive education and parental involvement in increasing children's risk awareness in Zimbabwe.

4.3. Model Equation

The following equation represents the logit regression model:

Logit(p) = -2.1604 + 2.4482(Age) + 6.0103(Education Level) + 5.1409(Access to Devices) + 3.0240(Frequency of Internet Usage) + 5.1386(Awareness of Online Safety Practices) + 1.6473(Guidance on Internet Usage) [1]

The logit regression analysis convincingly supports the importance of *Age, Education level, Access to devices, frequency of Internet Usage, Awareness of online safety* and *Guidance on Internet usage* as key factors influencing children's awareness of online risks in Zimbabwe. *Gender, Province* and *School attended* were insignificant; therefore, they were excluded from the model. These results provide a solid foundation for developing strategies to improve online safety awareness among children in Zimbabwe.

4.4. Demographic Factors on the Perceived Need for Online Safety Education

Based on the ANOVA results in Table 4 below, we can draw detailed conclusions regarding the impact of demographic factors on the perceived need for online safety education among children in Zimbabwe.

Table 3. ANOVA for Demographic Factors on the Perceived Need for Online Safety Education

	sum_sq	df	F	PR(>F)
C(Q("Gender"))	1.011310	1.0	3.054614	0.015239
C(Q("Age"))	3.130354	3.0	5.038809	0.001753
C(Q("province"))	6.025547	9.0	3.233029	0.343654

C(Q("education level "))	5.085639	5.0	2.200021	0.000000
C(Q("school attend "))	8.065341	20.0	5.222067	0.540654
Residual	9.036952	2603.0	NaN	NaN

The F-statistic for **Gender** is **3.0546** with a p-value of **0.0152**, which shows that gender is statistically significant (p < 0.05). This means that gender directly affects how children recognise the need for online safety education. The F-statistic for **Age** is **5.0388** with a p-value of **0.0018**, indicating a strong, statistically significant impact on the perceived need for online safety education. The F-statistic for **Province** is **3.2330** with a p-value of **0.3437**, suggesting that province does not impact the perceived need for online safety education. This means that geographical differences within Zimbabwe do not meaningfully influence how children perceive online safety. The F-statistic for **Education Level** is **2.2000** with a p-value of **0.0000**, demonstrating a highly significant impact of education level on the perceived need for online safety education. This shows that children at different educational levels perceive the necessity of online safety education differently, likely due to the varying levels of experience with online content and digital literacy training. The F-statistic for **schools attended** is **5.2221** with a p-value of **0.5407**; this means that the type of school attended does not significantly influence the perceived need for online safety education. In Zimbabwe, this finding shows that whether a child attends a public or private school does not considerably affect their perception of the need for online safety education. The residual sum of squares is relatively low, suggesting that the demographic factors in the model explain a significant portion of the variance in the perceived need for online safety education. However, it is essential to note that other variables not included in this model could also shape perceptions, such as socioeconomic status.

4.5. Children's Online Activities and Exposure to Online Risks

This study utilised the Chi-Square tests to explore the relationship between children's online activities and their exposure to online risks, providing essential insights into the factors that enhance or mitigate these risks**.**

Table 4. Chi-Square Test Results

Chi-Square Test	**Chi-Square Statistic**	**P-value**	**Degrees of Freedom**	**Significant Association?**
Virtual friend met online vs. Encountered threats or risks	3.7866	0.0357	2	Yes
Met someone face-to-face from the Internet vs. Encountered threats or risks	3.9835	0.0082	2	Yes
Frequency of encountering sexual content online vs. Seen websites or discussions on harmful topics	7.7566	0.0702	5	No
Use of social media vs. Encountered threats or risks	13.8250	0.0001	1	Yes

The Chi-Square test results show several critical insights into how children's online activities are linked to potential threats. The significant association between meeting virtual friends online and encountering risks, shown by a Chi-Square statistic of 3.7866 and a p-value of 0.0357, indicate that forming friendships online increases a child's vulnerability to online threats. This underscores the importance of guiding children in managing their online interactions. Similarly, the Chi-Square test between meeting someone face-to-face from the Internet and encountering risks shows a significant association, with a Chi-Square statistic of 3.9835 and a p-value of 0.0082. This result points to the dangers inherent in offline meetings with online friendships, which means such encounters considerably raise the risk of exposure to harmful situations.

The Chi-Square test between the frequency of encountering sexual content online and seeing websites on harmful topics shows a marginal association, with a Chi-Square statistic of 7.7566 and a p-value of 0.0702. Although the p-value is slightly above the traditional 0.05 threshold, the result indicates that children exposed to sexual content online are likely to encounter other forms of harmful content, such as discussions on dangerous behaviours. The extremely low p-value (p = 0.0001) shows an influential association between social media use and encountering online risks. This means that social media use is a significant predictor of exposure to online threats, highlighting the importance of monitoring and managing social media interactions to reduce risk. While social media enables connectivity and communication, it also exposes users to threats such as cyberbullying, phishing, misinformation, and privacy breaches. Social media platforms often involve sharing personal information and interactions with various individuals, including strangers. Additionally, the social pressure to engage in risky behaviours or share personal details online can increase vulnerability to threats, making social media a significant factor in the risks encountered online.

The outcomes of these Chi-Square tests highlight the complex dynamics of online interactions and the associated risks. The significant associations found in the tests suggest that certain online behaviours, such as forming online friendships, meeting Internet friends in person, and using social media, are associated with encountering online risks. These behaviours often involve a level of trust and exposure that can be exploited by malicious actors, leading to a range of adverse outcomes. These findings emphasize the importance of educating children about the potential risks of certain online behaviours. They also highlight the need for strong safety measures, privacy protections, and responsible digital behaviour to mitigate online risks.

5. Conclusions, Discussion and Recommendations

5.1. Conclusions

This study’s logit regression and Chi-square test results comprehensively assessed the factors influencing children’s awareness of online risks in Zimbabwe. The statistically significant relationships identified between demographic factors, children’s engagement in online activities, and exposure to online threats provide a complex view of the digital challenges faced by Zimbabwean children. Key findings highlight that older children who are better informed about the Internet and those who frequently use the Internet tend to be more cognizant of online dangers. However, the Chi-square test results underscore the tangible risks of meeting online friends in person, significantly increasing exposure to online threats.

5.2. Discussion

The implications of these findings are diverse. Firstly, the profound influence of educational initiatives on enhancing online safety awareness underscores the potential of targeted digital literacy programs as practical tools for promoting safer online behaviours. Nevertheless, the difference between children’s perceived online safety knowledge and their actual risk encounters indicates a pervasive overconfidence issue, warranting more practical and scenario-based approaches in digital literacy education. Furthermore, the limited role of parental awareness in influencing children’s comfort in discussing online experiences highlights the necessity for improved family communication strategies regarding online safety. The importance of parental participation in shaping children’s navigation of online spaces safely cannot be undermined.

5.3. Recommendations

a) *Digital Literacy Education*

There is a need to implement comprehensive digital literacy programs that teach elementary Internet skills and emphasise critical online thinking, threat detection, and practical risk management approaches. Incorporating digital literacy into school curricula from an early age should be encouraged, ensuring that children understand online risks as they grow.

b) *Parental Participation*

Educational workshops and resources should be developed for parents to deepen their knowledge of Internet dynamics and social media, hence training them to guide their children better. Open discussions about online encounters should promoted between children and parents, and schools or community centres may facilitate this to promote a helpful environment for sharing troubles and managing online communications effectively.

c) *Policy and Community Action*

Policymakers should be encouraged to craft regulations that foster safer online environments for children, including safe surfing choices and stricter mechanisms against online predators. Community Information Centres and non-profit organisations should also be mobilised to spearhead awareness programs and provide monitored online access points for children, ensuring safe Internet use under expert supervision.

d) *Research and Continuous Monitoring*

Ongoing research should be conducted to monitor changing trends in technology usage among Zimbabwean children and evaluate the impact of online safety initiatives. Regular evaluations of digital literacy programs in educational settings may be mandated, adjusting strategies based on student feedback and empirical data.

In summary, effectively addressing the challenges found in this study necessitates a cooperative strategy involving children, parents, educators, and the government. Promoting an informed community adept at managing the digital realm may significantly reduce the risks encountered by Zimbabwean children online. This proactive, inclusive approach secures individual safety and nurtures a generation of digitally literate individuals poised to succeed in a digital-global society.

Acknowledgements

The authors would like to extend their gratitude to the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) for its invaluable support and resources throughout the research process. We also acknowledge the Research and Development Department for their guidance, technical assistance, and unwavering commitment to ensuring the success of this study.

References

Allison, K. (2018). *Online Risks, Sexual Behaviors, and Mobile Technology Use in Early Adolescent Children: Parental Awareness, Protective Practices, and Mediation Early Adolescent Children*. University of South Carolina

Child Rights International Network (CRIN). (2019). *Children's rights and the digital environment: A global overview*. Retrieved from https://www.crin.org/en/library/publications/childrens-rights-and-digital-environment-global-overview.

Chingoriwo, T. (2022). Cybersecurity challenges and needs in the context of digital development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies*, 3(2), 77-104.

Dzingirayi, P. & Musemburi, L. (2023). The Quality of Secondary School-based Counselling Services in Contemporary Digitalised Learning Environment in Zimbabwe. *Zimbabwe Journal of Health Sciences (ZJHS),* 3(2).

Dzoro, J., Chereni, A., & Gwenzi, G. D. (2019). Internet risks and teenage children's agency: A case of post-primary students at a school in Chiredzi, Zimbabwe. *African Journal of Social Work*, 9(2), 87-96.

Global Internet Report 2022: The Future of the Internet. (2022). Internet Society. Retrieved from https://www.internetsociety.org/globalinternetreport.

Green, A., Wilkins, C., & Wyld, G. (2019). *Keeping Children Safe Online*. New Philanthropy Capital.

Hawkins, R. (2017). *The Relationship Between Teacher-Student Assignment and High School Student Equity in One North Carolina School District*. Dissertation paper for University of North Carolina at Chapel Hill Graduate School.

Lee, A. & Cook, P. (2014). The conditions of exposure and immediacy: Internet surveillance and Generation Y. *Journal of Sociology*, 51(3).

Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2017). *Children's online activities, risks and safety: A literature review by the UKCCIS Evidence Group*. ResearchGate.

Mabvurira, V. & Machimbidza, D. (2022). Cyberbullying among high school learners in Zimbabwe: Motives and effects. *African Journal of Social Work*, 12(3), 98-107.

Moyo, A., Tsokota, T., Ruvinga, C., & Chipfumbu Kangara, C. T. (2022). An e-safety framework for secondary schools in Zimbabwe. *Technology, Knowledge and Learning*, 27(4), 1133-1153.

Muhingi, W. N., Mavole, J. N., & Nzau, M. (2020). Stakeholders Awareness Creation on Online Child Abuse among Primary School Children in Langata Sub Country, Nairobi County, Kenya. *Journal of Research Innovation and Implications in Education*, 4(3), 210-213.

Mutunhu, B., Dube, S., Ncube, N., & Sibanda, S. (2022, April). Cyber security awareness and education framework for Zimbabwe universities: A case of National University of Science and Technology. In *Proceedings of the International Conference on Industrial Engineering and Operations Management Nsukka, Nigeria*, pp. 5-7.

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30(2).

Tsokota, T., Mhloza, V., & Chipfumbu-Kangara, C. T. (2022). A strategy to enhance e-safety among first-year students at Zimbabwean universities: action research. *Educational Technology Research and Development*, 70(2), 639-655.

UNICEF. (2021). *The State of the World's Children 2021: On My Mind - Promoting, protecting and caring for children's mental health*. Retrieved from https://www.unicef.org/reports/state-worlds-children-2021.

Yujin, J. & Ko, B. (2023). Online Safety for Children and Youth under the 4Cs Framework—A Focus on Digital Policies in Australia, Canada, and the UK. *Children*, 10(8).

Yuliana, Y. (2022). The Importance of Cybersecurity Awareness for Children. *Lampung Journal of International Law*, 4(1), 41-48.

Zimbabwe Report. (2020). Global Kids Online. Retrieved from https://globalkidsonline.net/zimbabwe.