Scientific Research Publishing

Intelligent Information Management, 2023, 15, 350-372
https://www.scirp.org/journal/iim
ISSN Online: 2160-5920
ISSN Print: 2160-5912

Investigating How Parental Perceptions of Cybersecurity Influence Children's Safety in the Cyber World: A Case Study of Saudi Arabia

Tariq Saeed Mian*, Eman M. Alatawi

Department of IS, College of Computer Science and Engineering, Taibah University, Madinah Almunwarah, Saudi Arabia
Email: *tmian@taibahu.edu.sa, eatawi@taibahu.edu.sa

How to cite this paper: Mian, T.S. and Alatawi, E.M. (2023) Investigating How Parental Perceptions of Cybersecurity Influence Children's Safety in the Cyber World: A Case Study of Saudi Arabia. *Intelligent Information Management*, **15**, 350-372.
https://doi.org/10.4236/iim.2023.155017

Received: August 18, 2023
Accepted: September 8, 2023
Published: September 11, 2023

Abstract

This paper explores the convergence of Saudi Arabia's Vision 2030 with the increasing dependence on the Internet for educational purposes. It sheds light on the potential cybersecurity risks and how parental perception impacts children's willingness to adapt cybersecurity features. By instilling the significance of cybersecurity awareness in early stages, society can provide children with the necessary skills to navigate the digital realm responsibly. As we progress, ongoing research and collaborative endeavors will be pivotal in formulating effective strategies to shield the digital generation from the potential pitfalls of the virtual realm. Regular Internet usage is essential for various purposes such as communication, education, and leisure. The cohorts of Generation Z and Alpha were born during a period of exponential Internet growth, leading them to heavily engage with the Internet. Consequently, they are equally vulnerable to cybersecurity threats just like adults. Addressing potential security risks for today's youth becomes the responsibility of parents as the primary line of defense. This research focuses on raising awareness about the imperative of ensuring children's safety in the online sphere, particularly by their parents. The study is conducted within the specific context of Saudi Arabia, aiming to examine how Saudi parents' perception of cybersecurity influences their children's cyber safety. The study identifies critical factors, including attitudes towards cybersecurity, awareness of cybersecurity, and prevailing social norms regarding cybersecurity. These factors contribute to the development of parents' intention to prioritize cybersecurity, which consequently affects their children's behaviors in the digital realm. Utilizing a quantitative approach based on a questionnaire, the study employs a Structural Equation Modeling (SEM) framework to analyze the collected data. The study's findings underscore that parents' intent towards cybersecurity plays a significant role in shaping their children's behavior concerning cyber safety.

Keywords

E-Learning, Cybersecurity, Saudi Arabia, Saudi Vision 2030, Cybersecurity Awareness, Parenting in Cyber Era, Adolescence

1. Introduction

Saudi Arabia's Vision 2030 is an ambitious and comprehensive blueprint aimed at diversifying the country's economy, reducing its dependency on oil, and fostering socio-economic development across various sectors. One significant aspect of this transformation is the emphasis on leveraging the power of the Internet and digital technology to reshape education. The integration of technology and the reliance on the Internet for education align with the broader goals of Vision 2030 to create a knowledgeable, skilled, and globally competitive workforce. This article delves into how Saudi Arabia's Vision 2030 intersects with the growing reliance on the Internet for education, highlighting the opportunities and challenges this digital transformation presents.

Saudi Arabia Vision 2030 aims to diversify the Saudi economy, enhance the quality of life for citizens, and position the nation as a global hub for innovation, trade and investment. Historically reliant on oil revenue, Saudi Arabia recognized the need to diversify its economy in the face of fluctuating oil prices. The vision outlines initiatives to foster non-oil sectors such as tourism, entertainment, healthcare, and technology. The creation of new economic zones, such as NEOM and Qiddiya, is a testament to this commitment. This diversification strategy is aimed at reducing the country's dependence on oil, stimulating innovation, and creating job opportunities for its youthful population (Saudi Vision 2030, 2016). Central to the vision is the aspiration to enhance the quality of life for Saudi citizens. The National Transformation Program, an integral component of Vision 2030, focuses on improving healthcare services, education, infrastructure, and social development. By investing in these areas, the government aims to create a more vibrant and attractive living environment, ensuring that citizens have access to world-class services and opportunities. [1]

The cornerstone of Saudi Vision 2030's digital economy focus lies in its goal of reducing the country's dependence on oil revenue by diversifying its economic base. The digital economy presents an avenue for growth and innovation across various sectors. By investing in digital infrastructure, fostering innovation, and promoting entrepreneurship, Saudi Arabia aims to create a vibrant ecosystem that supports emerging industries, such as e-commerce, Fintech, and tech startups [2]. The digital economy is synonymous with innovation, and Saudi Arabia recognizes this as a key driver of economic growth. Vision 2030 encourages the development of a culture of innovation by nurturing startups, creating incubators and accelerators, and supporting research and development initiatives. The establishment of tech parks, such as the King Abdullah University of Science and Technology (KAUST), serves as a testament to the commitment to fostering technological advancements [3]. Vision 2030 aims to enhance efficiency and transparency through the digital transformation of society.

The digital economy aligns seamlessly with the ambition of creating a knowledge-based economy in Saudi Arabia. The emphasis on education, research, and technology transfer is integral to nurturing a skilled workforce that can drive digital innovation. The focus on developing Saudi human capital, particularly in STEM fields, positions the nation to take advantage of the digital revolution [4].

It is a fact that the Internet has intricately woven itself into every facet of our lives [5]. It has profoundly transformed how we engage with various activities, including shopping habits, dietary choices, connecting with loved ones, forming new relationships, and even immersing ourselves in cinematic experiences [6]. The introduction of digital technologies to children commences at an early age, with data from 2013 revealing that a substantial 75% of American children below nine years old were already utilizing tablets or smartphones within their homes [7]. This trend has endured, evident by 2018 figures in the United Kingdom showing a significant proportion of young individuals owning personal tablets, with 42% of 5 to 7-year-olds and 47% of 8 to 11-year-olds falling into this category [8]. Even with age restrictions on popular social networking sites, a disconcerting trend emerged in 2018, with 12% of nine-year-olds in most EU countries partaking in these platforms [8]. This trend is mirrored in Saudi Arabia, a nation that follows the global acceptance of cyberspace across various demographic groups.

According to the "Internet World Stats" 2021 report, approximately 73% of the Saudi Arabian population had access to the Internet [9]. The trend of young children and teenagers increasingly utilizing the Internet is observable in Saudi Arabia. A substantial portion of these young users employ the Internet for educational purposes, social networking, entertainment, and gaming. Ofcom's latest report on Internet users aged 9 to 15 in Saudi Arabia revealed a strong presence of young individuals in digital spaces. The report underscores that a significant number of children in this age range are active Internet users, exploring the digital realm and its diverse offerings. Notably, the report emphasizes that a considerable percentage of 9 to 15-year-olds in Saudi Arabia have Internet access through various devices such as smartphones, tablets, and computers. This trend aligns with the global pattern of growing digital engagement among young individuals. However, alongside increasing Internet penetration and children's online presence comes the associated risk of cybercrime and cybersecurity challenges. Children are susceptible to various online threats, including cyberbullying, exposure to inappropriate content, and potential exploitation by malicious entities. Ensuring their online safety and fostering cybersecurity awareness among children and parents have become essential responsibilities.

The growing reliance on cyberspace can lead to a surge in cyber violations. As highlighted by [10], the rapid advancement of new technologies, digital platforms, immersive software, and evolving media behaviors is surpassing our comprehension of their impact on Internet users' well-being. Consequently, among all Internet users, children are the most vulnerable to cybercrime, including cyberbullying, scams, interactions with strangers, and exposure to inappropriate content such as pornography and hate speech [11]. These significant threats to cybersecurity and well-being faced by children in the online sphere can lead to severe consequences for their mental health, as emphasized by [12]. As Saudi Arabia's digital landscape continues to evolve, it becomes increasingly imperative to implement measures that protect children from the risks of the virtual world.

In the realm of children's Internet usage, it's evident that many parents may not fully comprehend the crimes and dangers prevalent in cyberspace. However, it is their responsibility to oversee and regulate their children's online activities [13]. Home remains a significant setting for Internet use, underlining the crucial role parents play in safeguarding their children from cyber threats. Various studies highlight the positive impact of parental supervision on children's development, spanning both the pre-Internet era and the present digital age [14]. Parents need to adapt their supervisory role to the digital age, as the risks in cyberspace hold the same importance and present considerable challenges. Regrettably, many parents lack full awareness of their children's online activities and lack adequate knowledge about the potential cyber threats their children might encounter [15]. While some parents are aware of parental control features, only a small percentage effectively utilize them. Moreover, widely used social media platforms often lack proper parental control settings, exacerbating the complexity of the issue.

The integration of Information and Communication Technology (ICT) in schools aims to enhance adolescents' digital skills and critical thinking. However, this initiative is often marred by the lack of cybersecurity and privacy awareness among children and parents. Consequently, a significant number of children venture into cyberspace without appropriate parental guidance, rendering them vulnerable to cybersecurity threats [16]. Studies indicate that a substantial number of European children and young individuals have also experienced cyber threats while using the Internet. Thus, this issue is not unique to Saudi Arabia. Parental involvement and awareness play a pivotal role in shielding children from cyber risks in the digital age. Parents must actively engage in their children's online activities, utilize available parental control tools, and cultivate a culture of cybersecurity awareness to ensure a safer digital experience for children globally [17].

Recent findings reveal that one out of four children have encountered cybersecurity threats on the Internet [18]. This statistic underscores that a considerable number of children are using cyberspace on mobile devices with limited parental control, thereby exposing them to cybersecurity threats. Given the gravity of this issue, researching ways to protect children from cybercrime is crucial

[19]. It's important to note, however, that the current research on children and cybersecurity is predominantly focused on Anglo-American contexts. Additionally, most research predominantly addresses children's safety, security, and privacy in cyberspace.

Conversely, there's a lack of research concerning parental cybersecurity behaviors, such as online restrictions, and their awareness of their child's online behavior related to cybercrime, like cyberbullying. To bridge this gap, further research is needed to explore and understand the role of parents in mitigating cyber threats faced by children. This research should extend beyond Western countries to encompass diverse cultural contexts, such as KSA and other GCC regions, where Internet usage patterns and cyber risks may vary. By broadening the research scope and examining the issue from multiple perspectives, policymakers and parents can gain valuable insights into effective strategies to protect children from cyber threats and create a safer online environment for them.

2. Saudi Vision 2030: Transforming Education through Internet Reliance

Saudi Arabia's Vision 2030 is an ambitious blueprint aimed at diversifying the country's economy, enhancing the quality of life for its citizens, and reducing its dependence on oil. One of the critical pillars of this vision is the transformation of the education sector to align with the demands of the 21st century. A significant aspect of this transformation is the reliance on the Internet for education, which has the potential to reshape the way knowledge is accessed, disseminated, and acquired. This article delves into the Saudi Vision 2030's emphasis on leveraging the Internet for educational advancement, highlighting its impact, benefits, and challenges [20].

The Internet has ushered in a paradigm shift in education by breaking down traditional barriers of access to information. Saudi Arabia recognizes the power of the Internet as a tool to provide quality education to its citizens regardless of their geographical location. With over 70% of the population under the age of 30, the nation's young demographics stand to benefit significantly from this technological shift [21].

One of the cornerstones of Saudi Vision 2030 is the development of online learning platforms and digital resources. These platforms offer a range of benefits, including flexibility in learning schedules, access to diverse educational materials, and the opportunity for self-paced learning. The King Abdulaziz and His Companions Foundation for Giftedness and Creativity (*Mawhiba*), for instance, have introduced numerous online programs to nurture gifted students across the nation [22].

Saudi Vision 2030 has also catalyzed the establishment of e-learning initiatives that cater to different levels of education, from primary to tertiary. The Ministry of Education's (MoE) Tatweer program, for example, focuses on developing and implementing digital solutions to enhance the learning experience. Such initiatives not only enable students to access high-quality education but also empower educators to employ innovative teaching methods and interactive content [23].

While the integration of the Internet into education presents a plethora of advantages, it also comes with challenges that need to be addressed effectively. Digital literacy is crucial in ensuring that students and educators can make the most of online resources. Ensuring equitable access to the Internet and appropriate devices across all regions, socioeconomic backgrounds, and communities is also essential to avoid creating a digital divide [24].

The shift towards Internet-reliant education in line with Saudi Vision 2030 offers a multitude of benefits. It allows for personalized learning experiences, accommodating various learning styles and paces. Students gain access to a wealth of resources, including online libraries, research databases, and educational videos, fostering independent research skills. Additionally, the integration of technology equips students with digital literacy skills essential for the modern workforce.

The Saudi Vision 2030's emphasis on Internet reliance for education reflects a forward-looking approach to preparing the nation's youth for the challenges and opportunities of the digital age. By leveraging the power of the Internet, Saudi Arabia aims to democratize education, empower learners, and develop a future-ready workforce. While challenges like cybersecurity, digital inclusion and balanced learning approaches need to be addressed, the potential impact of Internet-enabled education on Saudi Arabia's socio-economic landscape is undeniably promising. As the country continues to navigate this transformative journey, collaboration between educational institutions, policymakers, and technology providers will be pivotal in realizing the full potential of this vision.

3. Theoretical Foundation

In the realm of comprehending human behavior in response to perceived threats, the Protection Motivation Theory (PMT) emerges as a robust and insightful framework [25]. This theory delves into our reactions when confronted with threats, drawing from our assessments of potential dangers and available coping mechanisms [26]. Consequently, the PMT comprises two pivotal aspects: threat appraisal and coping appraisal, both of which shape our protection motivation and responses to threats. Threat appraisal centers on an individual's evaluation of the risk level involved. Within the scope of our research, this pertains to how parents assess the risks their children might face in the cyber world. This component is further subdivided into two elements: perceived vulnerability and perceived severity of the risk. On the other hand, coping appraisal pertains to our capacity to manage the identified risk, akin to the concept of self-efficacy [27].

When confronted with a potential threat, our initial step is to gauge its severity and vulnerability. If both aspects are deemed high, the threat assessment intensifies. Following this evaluation, we move on to analyze the available coping strategies to effectively address the threat. Investigating the influence of parental cyber security behavior on a child's digital well-being is the central focus of this contemporary inquiry. This endeavor encompasses the amalgamation of prominent frameworks, notably the Protection Motivation Theory (PMT), as we seek to unravel the complexities of the observed phenomenon.

The Protection Motivation Theory (PMT) sheds light on the intricate interplay between threat appraisal, coping appraisal, and protection motivation in the face of perceived threats. Gaining insight into these cognitive processes allows us to grasp human behavior regarding information and cyber security. As technology continually evolves, embracing good cyber hygiene practices becomes a fundamental aspect of ensuring a secure digital future.

3.1. Children's Online Safety and Parental Attitudes: A Crucial Nexus

The rapid proliferation of digital technology and the Internet has revolutionized the way children interact, learn, and entertain themselves. However, this technological advancement has also brought forth concerns about children's online safety. As youngsters increasingly engage with online platforms, the role of parents in shaping their online experiences becomes pivotal. This paper delves into the landscape of children's online safety, focusing on parental attitudes and their significance in ensuring a secure digital environment for young users.

The Internet has transformed from a niche tool to an indispensable aspect of modern life. Children today grow up in a digital world where they effortlessly navigate various online platforms, from social media to educational websites. While the Internet offers numerous opportunities for learning and exploration, it is accompanied by risks such as cyberbullying, exposure to inappropriate content, and online predators.

Parental attitudes play a pivotal role in children's online safety. A study by Livingstone and Haddon [28] emphasized that the involvement of parents in their children's online activities is vital for their protection. Positive parental attitudes, including open communication and active monitoring, have been linked to a decrease in risky online behavior among children [29].

Despite recognizing the importance of online safety, parents often face challenges in effectively safeguarding their children. A study by Albury and Crawford [30], highlighted that parents struggle to keep up with rapidly evolving digital trends, leading to a "digital disconnect" between them and their tech-savvy children. This gap can hinder parents' ability to comprehend the potential risks their children face online.

To bridge this gap, educational initiatives are imperative. Schools and organizations should provide parents with resources to enhance their digital literacy, enabling them to better understand the online landscape. Programs like workshops and webinars can empower parents to engage in constructive conversations with their children about online safety.

In addition to education, technological solutions can aid parents in ensuring their children's online security. Parental control apps and content filters offer a practical way to restrict children's access to inappropriate content. A study by Garmendia, *et al.* [31] found that parents who employed such tools felt more confident in managing their children's online experiences.

The challenge lies in striking a balance between allowing children the freedom to explore the digital world and ensuring their safety. Overbearing restrictions might hinder a child's ability to develop critical digital skills and navigate online challenges independently. Therefore, parents must adopt an approach that fosters autonomy while providing a safety net.

3.2. Children and Cybersecurity

In today's interconnected world, where digital technology is an integral part of daily life, children are exposed to a myriad of online opportunities and risks. The evolution of cyberspace has led to an increased reliance on technology, making cybersecurity a critical concern, especially for the younger population. As children navigate the digital landscape, their exposure to cyber threats necessitates a comprehensive understanding of the impact of cybersecurity on their well-being and development. This article explores the multifaceted influence of cybersecurity on children, highlighting both the challenges they face, and the measures required to ensure their online safety.

Children are susceptible to a variety of cyber threats, ranging from online predators and cyberbullying to exposure to inappropriate content. A study conducted by [32] revealed that nearly 15% of adolescents have experienced online harassment, while 6% have been targets of cyberbullying. Such experiences can lead to emotional distress, anxiety, and even depression, adversely affecting children's mental health and overall well-being [33].

The proliferation of social media platforms has intensified these risks, with children often oversharing personal information without understanding the potential consequences. Moreover, the rise of "stranger danger" in virtual spaces necessitates the development of strong cybersecurity habits, including protecting personal information and practicing safe online interactions.

Addressing these challenges requires a collaborative effort from parents, educators, and policymakers. Schools play a crucial role in providing cybersecurity education to children, teaching them about online ethics, privacy protection, and responsible online behavior. By integrating cybersecurity into curricula, children can become informed digital citizens, equipped to make safe and ethical choices online [34].

Empowering children with the skills to recognize and respond to cyber threats not only reduces their vulnerability but also fosters a sense of agency and confidence in the digital realm. As stated by [35], when children understand how to protect themselves online, they are more likely to report incidents of cyberbullying or suspicious behavior, creating a safer online environment for all.

Technological solutions also play a significant role in enhancing children's cybersecurity. Parental control software and filtering tools can help parents manage their children's online experiences, ensuring age-appropriate content and curbing exposure to potential risks. Furthermore, open communication between parents and children about their online activities fosters trust and enables parents to guide their children effectively [36].

3.3. Key Factors Influencing Cybersecurity Intentions

The proliferation of new technologies like AI, IoT, and cloud computing broadens the risk of cyber-attacks. The integration of household devices and the excessive use of communication and social media applications have opened new avenues for cyber-attacks. Similarly, cybersecurity intentions are influenced by several crucial factors that drive individuals to prioritize cybersecurity. Intentions are a combination of consciously held beliefs, feelings, motivations, and desires. They serve as catalysts for our choices and behaviors. However, intention towards cybersecurity is composed of various factors. These elements are now under investigation in relation to parental cybersecurity behavior in the following sections.

Attitudes can be developed through the socialization process, which involves transmitting cultural norms, values, and beliefs. Eagly and Chaiken [37], found that attitudes are formed through a combination of cognitive (information processing) and affective (emotional responses) processes. Several factors, including family, friends, the media, and personal experiences, influence these processes. Similarly, attitudes toward cybersecurity are influenced by a variety of interrelated factors that impact both cognitive and affective processes. Hence, parents' attitudes toward cybersecurity can shape their children's Internet experiences, as suggested by [38]. Consequently, attitudes that prioritize children's safety and well-being in the digital world may begin to emerge.

A person's attitude toward cybersecurity is shaped by their ideas, emotions, and past experiences [39]. Thus, an Internet user with knowledge of potential risks associated with cyberspace will set limits on their usage. Similarly, a parent's approach or attitude towards their child's Internet safety determines their child's actions or behavior [40]. Therefore, parents' attitudes toward their kids' online safety undeniably influence their desire to keep them secure. Methods of monitoring children's online activities vary by culture, society, and country. Some parents have immense faith in their children's ability to use the Internet appropriately. Instead of enforcing stringent restrictions, they promote open communication and equip their kids with the tools to make wise online decisions [41]. Conversely, some parents adopt a more cautious approach, placing greater emphasis on parental oversight and management of their children's online activity.

A proactive parenting approach acts as a catalyst, motivating parents to safeguard their children's Internet experiences. Parents who are supportive of cybersecurity exhibit a comprehensive understanding of the digital world and its potential hazards. Monitoring a child's online activities is one example of how positive cybersecurity attitudes translate into practical actions [42]. Despite the potential intrusiveness, parents with a positive outlook view monitoring as a tool for guidance rather than surveillance. This approach fosters an environment of open communication, where children feel comfortable discussing their online experiences. Based on this discussion, this study hypothesized that:

In tandem with this, social norms driven by society, norms, and interpersonal relationships exert significant influence on individuals' behavior. In the realm of cybersecurity and technological acceptance, individuals often grapple with external influences and beliefs that shape their conduct. The impact of social pressures on parents' behavior concerning their children's online safety gains greater significance as cybersecurity becomes more critical and children spend more time online. The pivotal role of subjective norms in shaping human behavior, particularly in the context of cybersecurity, has been extensively explored in previous research. The significance of subjective norms in influencing technological acceptability and adherence to cybersecurity measures was highlighted by [43] [44]. These expectations, shaped by peer pressure and societal standards, significantly influence online behavior. A parent's behavior regarding their child's online safety could be influenced by societal pressures (*i.e.*, monitoring a child's Internet usage).

While the widespread use of the Internet provides unparalleled opportunities for learning and discovery, it also introduces a range of cyber hazards. Children are particularly vulnerable to online predators, cyberbullying, and inappropriate content due to their curiosity and lack of experience. According to [45], the digital environment poses a significant threat to children's core beliefs and self-identity. Hence, parental awareness of the dangers is crucial. Parents must recognize potential risks posed by the online environment and take proactive steps to protect their children. Parental cybersecurity knowledge is needed to safeguard children's digital well-being and gain a comprehensive understanding of cyber threats [46].

Education is the first step in raising parental cybersecurity awareness. Parents who are educated about the different online threats they and their children face, such as cyberbullying, identity theft, and exposure to explicit material, tend to prioritize their children's cybersecurity. Informed parents can help their children develop responsible online behavior and proactively handle any hazards [47]. Children's online safety heavily depends on parental engagement and guidance. Parents who are well-versed in cybersecurity issues can educate their children about risks and provide them with the tools they need to use the Internet safely. Conversations about responsible social media use, safeguarding personal information, and treating people with respect online influence the development of a child's positive digital footprint.

Open communication is a vital component of parental cybersecurity awareness. When parents establish a trusting relationship with their children, children feel more comfortable discussing their online experiences and concerns. This open communication empowers children to seek guidance if they encounter uncomfortable situations or encounter unfamiliar online content.

3.4. The Nexus between Cybersecurity Intention and Behaviour towards Child Cyber Wellbeing

The intention is a culmination of several factors, such as attitudes, social norms, and awareness. Cultivating positive attitudes toward cybersecurity through responsible behavior and risk awareness is crucial. Parents' intention to prioritize children's online safety hinges on their attitudes, social influences, and level of cybersecurity awareness. Parental intentions to safeguard children's online well-being are intricately linked to the dynamic interplay between their cybersecurity attitudes, societal pressures, and awareness. An individual's actions in the digital realm are fundamentally grounded in their attitude toward cybersecurity. Positive attitudes correlate with favorable behaviors in cybersecurity contexts. Conversely, unfavorable attitudes can lead to unsafe behaviors that jeopardize children's online safety [48].

Social pressure significantly shapes human behavior. One's approach to cybersecurity can be influenced by the need to conform to digital norms. Social expectations often drive individuals to adopt practices aligned with the prevailing digital culture. Equipping individuals with knowledge about potential threats and effective cybersecurity practices enhances their ability to ensure children's online safety and make informed decisions.

Parental active cybersecurity behavior refers to the proactive and aware steps parents take to safeguard their children's online well-being. Rooted in the protection motivation theory, people are inclined to take preventive measures when they perceive a threat and believe those measures will be effective. Parents who actively practice cybersecurity set positive examples for their children, promoting responsible behavior and underscoring the importance of taking precautions against online threats. Parental initiatives underscore the significance of security in the digital realm, thereby fostering a culture in which children appreciate sound online safety practices and are more likely to adhere to them.

Building on the aforementioned discussion, this study comprehends that (**Figure 1**):

H1: The attitude of parents towards cybersecurity significantly impacts their intention to prioritize their child's cybersecurity.

H2: Societal norms regarding cybersecurity significantly impact their intention to prioritize their child's cybersecurity.

H3: Parents with cybersecurity awareness are more inclined to prioritize their child's cybersecurity.

H4: Behaviors related to child's cybersecurity are more likely to be influenced by the intention to prioritize child's cybersecurity.

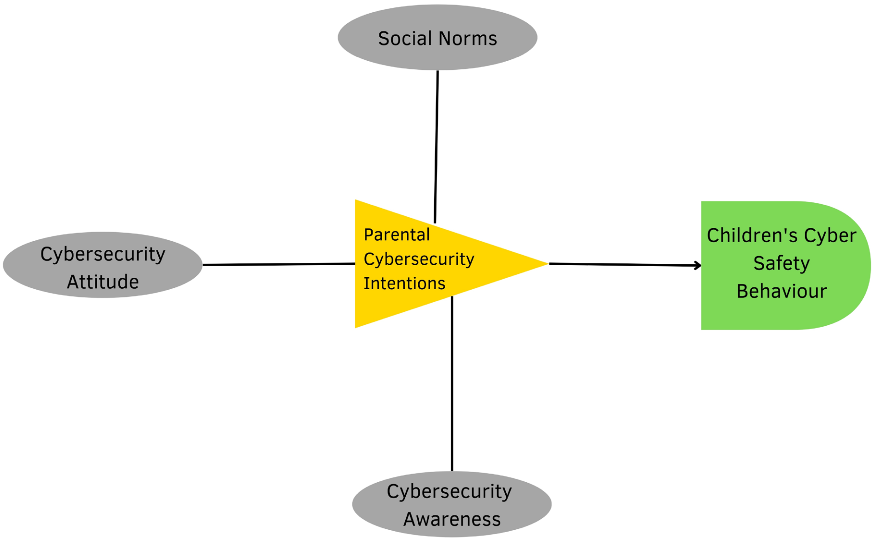
Social Norms
Cybersecurity Attitude
Parental Cybersecurity Intentions
Children's Cyber Safety Behaviour
Cybersecurity Awareness

Figure 1. Theoretical framework.

4. Methods and Materials

The objective of the present study is to empirically understand the factors that impact parents' cybersecurity intentions and, consequently, their behavior towards ensuring the online safety of children. This study utilized a cross-sectional design and employed a survey technique to gather pertinent data. Additionally, for data analysis, structural equation modeling was employed.

Measurement Model

The survey questionnaire was employed in the current study for data collection. A five-point Likert scale was utilized in the questionnaires to gather quantitative data. The constructs' items used in this study were adapted from previous works by [49] [50] [51].

The study's sample was selected using convenience sampling techniques. The sample size was determined using the formula $n = z^2 * (p * q) / d^2$, which is commonly used for qualitative variables in prevalence or cross-sectional studies. In this formula, "*n*" represents the sample size, "*p*" denotes the estimated proportion of the study variable or construct based on pilot studies, and "*d*" stands for the error, set at 5% for our case. "*z*" represents the Z-score, which is 1.96 for a 5% level of significance in our situation.

The gleaned data was analyzed using Structural Equation Model (SEM). Structural Equation Modeling (SEM) is a powerful statistical methodology used to analyze complex relationships among variables. It offers a comprehensive framework that allows researchers to examine both the direct and indirect relationships between variables within a single model. This essay provides an overview of SEM, its components, and its applications in data analysis. [52].

Structural Equation Modeling is a robust and flexible methodology that plays a crucial role in uncovering complex relationships within datasets. Its ability to integrate measurement and structural models makes it a valuable tool across various fields. By allowing researchers to test complex theories and hypotheses, SEM contributes significantly to advancing our understanding of intricate phenomena, as required in this research [53].

The study employed Partial Least Squares Structural Equation Mode (PLS-SEM). Partial Least Squares Structural Equation Modeling (PLS-SEM) is a statistical methodology used for analyzing complex relationships among variables in a structural equation modeling framework. PLS-SEM is particularly suitable when dealing with latent constructs, small sample sizes, and non-normal data distributions. This methodology integrates components of both regression analysis and factor analysis to provide insights into causal relationships, mediation, moderation, and latent variable interactions [52].

Partial Least Squares Structural Equation Modeling (PLS-SEM) is a flexible and powerful statistical methodology that facilitates the exploration of complex relationships among variables. Its suitability for small sample sizes, non-normal data, and predictive modeling makes it a valuable tool in various research domains. Researchers across disciplines can utilize PLS-SEM to uncover intricate patterns, validate theoretical models, and gain insights into causal relationships among latent constructs. PLS-SEM's robustness in handling small sample sizes and its ability to handle non-normal and even categorical data make it a suitable statistical approach for current research.

5. Results and Discussions

5.1. Descriptive Analysis

Table 1 presents the findings from the descriptive analysis of the sample's demographic characteristics.

Table 1. Descriptive analysis.

	Categories	Percentage
Gender	Male	78%
	Female	22%
Age	25 - 30	23%
	31 - 40	37%
	41 - 50	28%
	51 and above	12%
Education	High School and Below	18%
	Bachelors	52%
	Masters	25%
	PhD	5%

5.2. Validity and Reliability of Instrument

To assess the internal consistency among respondents, a reliability analysis was conducted, with Cronbach's alpha calculated for each variable. The obtained Cronbach's alpha values demonstrate that all variables fall within the acceptable range, surpassing the threshold of 0.7.

In the context of this study, construct validity and reliability analysis pertain to ensuring the data collection instrument aligns coherently with the research's objectives and goals. This assessment aims to validate that the items within the data collection instrument effectively measure the concepts outlined within the theoretical framework. The evaluation of construct reliability, which pertains to internal consistency, is determined using both Cronbach's alpha and composite reliability (with a threshold of 0.60). Similarly, the measurement of construct validity is gauged through average variance extracted (AVE), with a threshold of 0.50 [54]. The outcomes of the construct validity and reliability analysis are presented in **Table 2** below.

Moreover, the evaluation of construct validity involves the calculation of AVE (average variance extracted). The standard benchmark for AVE stands at 0.50. The outcomes of the AVE analysis are presented in **Table 3**, revealing that all variables have successfully met or surpassed the prescribed threshold.

To establish the distinctiveness of variables and their capacity to assess a phenomenon requires discriminant validity analysis. When performing discriminant analysis, the Fornell Larcker criteria is a potent tool that helps reveal how much a variable differentiates from others. It includes evaluating the correlations between variables with the square root of the average variance extracted (AVE) for each variable. A variable's AVE needs to be higher than the squared correlation with other variables to have discriminant validity [55]. The findings unequivocally demonstrate that each variable is distinct and measures a distinct collection of occurrences.

5.3. Partial Least Structural Equation Modelling

The present study has employed partial least squares-structural equation modeling (PLS-SEM) to conduct the measurement analysis of the gathered data. The outcomes of the measurement model analysis are displayed below. In order to elucidate the extent to which the dependent variable's variance is explained by the independent variable, the coefficient of determination (R2) is computed and presented in **Table 4**. Notably, the variables "Intention to Cybersecurity (ITC)" and "Behavior towards Child's Wellbeing (BTC)" exhibit significant R2 values.

The independent variables, namely Attitude towards cybersecurity, Awareness of cybersecurity, and social norms, collectively contribute to a significant 53.0% of the variance in the intention for child's cybersecurity. Likewise, the Intention toward child's cybersecurity variable contributes to a variance of 19.6% in the behavior towards child wellbeing (see **Table 5**).

Table 2. Construct reliability measurement.

Variables	Cronbach's Alpha	Remarks
Attitude Towards Cybersecurity (ATC)	0.78	Good
Awareness of Cybersecurity (AC)	0.82	Good
Social Norms (SN)	0.75	Good
Intention Towards Cyber Security (ITC)	0.81	Good
Behavior Towards Children's Wellbeing (BTC)	0.899	Good

Table 3. Construct validity measurement.

Variables	AVE	CR	Remarks
ATC	0.68	0.85	Good
AC	0.56	0.78	Good
SN	0.61	0.89	Good
ITC	0.72	0.82	Good
BTC	0.58	0.79	Good

Table 4. Discriminant validity.

Variables	ATC	AC	SN	ITC	BTC
ATC	0.871				
AC	0.889	0.883			
SN	0.824	0.793	0.808		
ITC	0.791	0.834	0.752	0.971	
BTC	0.848	0.935	0.744	0.864	0.921

Table 5. Model fitness.

Variables	R Square	R Square Adjusted
ITC	0.530	0.536
BTC	0.196	0.194

The structural model analysis was conducted using bootstrapping with 5000 iterations. The outcomes are showcased in Table 6, revealing that all coefficients hold significant values.

This research is aimed to explore the underlying motivating factors behind parental aspirations by investigating the relationships between attitudes toward cybersecurity. Parents' actions wield a significant influence on their children's perception of the online world, as they strive to cultivate a positive digital environment. Intentions serve as the fundamental drivers of parental behavior in safeguarding children's online safety. A multitude of interconnected variables,

Table 6. Path analysis.

Path Analysis	Co-Efficient	Standard Deviation	T Statistic	p Values	Decision
ATC → ITC	0.382	0.052	3.437	0.001	Supported
AC → ITC	0.673	0.009	28.347	0.000	Supported
SN → ITC	0.476	0.035	9.231	0.000	Supported
ITC → BTC	0.983	0.062	19.925	0.000	Supported

intricately tied to parents' evaluations of their children's digital realm, contribute to intention-driven actions. The emotional stance a parent adopts regarding their child's online safety profoundly shapes their conduct. Positive sentiments encourage parents to take proactive steps, engage in open discussions, and dedicate time to understanding Internet platforms.

Our data analysis reveals that parental attitude, awareness, and social norms concerning cybersecurity play pivotal roles in shaping parental intentions towards their children's online well-being. All three variables exhibit significant p-values (0.001, 0.000, 0.000) at a 95% confidence level. However, the beta coefficients elucidate that awareness of cybersecurity holds greater influence over the intention for cybersecurity. This highlights the phenomenon that parents possessing an attitude towards cyber security and an awareness of cyber threats are more inclined towards prioritizing their children's safety.

The expanding recognition of cyber wellness, advocated by various stakeholders including governments, societies, and educational institutions, has spurred a heightened sense of responsibility among parents to proactively ensure their child's online safety. Awareness stands as the foundational step in the journey to protect children's online well-being. When parents grasp the potential ramifications of prevalent social and security issues in the digital realm, they are more likely to be vigilant and motivated to provide heightened protection.

The impact of awareness on shaping security-related intentions cannot be overstated. Awareness and the intention to prioritize cybersecurity exhibit a positive correlation. This enhanced knowledge has prompted parents to take preventative actions in securing their children's online experiences. Collaborative efforts between governments, society, and educational institutions have equipped parents with the knowledge and tools necessary to foster a secure online environment. Workshops, seminars, and awareness initiatives have empowered parents to guide their children through the complexities of the digital world.

The research posited a direct relationship between parental cybersecurity intention and their commitment to safeguarding their children's online safety. This assertion gains empirical support through the utilization of structural equation modeling, yielding a significant t-statistic value. The measured path coefficient of 0.983 underscores a robust and positive connection between parents' intentions to protect their children online and their tangible online safety behaviors.

Consequently, it is plausible to argue that parents' heightened desire to shield their children from online threats translates directly into the proactive measures they adopt. This realization serves as a pivotal catalyst in achieving the overarching goal of ensuring children's online safety. This proposition is substantiated by substantial evidence.

6. Results and Discussions

Saudi Vision 2030 envisions a transformed education landscape, with eLearning as a pivotal tool. This ambitious initiative aims to leverage digital platforms to enhance accessibility, quality, and innovation in education, empowering Saudi citizens with skills for the future and fostering a knowledge-driven society. [56]

The intricate implications of cybersecurity on children's well-being necessitate a comprehensive approach involving multiple stakeholders. In an era characterized by digital advancements, the horizon is replete with opportunities for children's learning and personal development. Yet, amid these prospects, a host of challenges loom, posing threats that extend beyond the digital realm to affect children's mental, emotional, and physical health. As the landscape of cyber threats continually morphs, an imperative emerges to adopt a proactive strategy, one that synergizes education, empowerment, and technological innovation, to erect a fortified bastion of safety for our young digital denizens.

Recent investigations into this realm have assumed paramount importance, serving as the foundational building blocks upon which the edifice of cyber safety and security for the next generation rests. This article embarks on a journey through these recent revelations, poised to reshape not only the trajectories of researchers and practitioners but also the very landscape of children's online safety. As it unravels the multifaceted dimensions of this domain, the study rekindles a new perspective, prompting academicians to delve deeper, scrutinize rigorously, and refine models to cater to diverse contexts. Within this unique framework, the study awakens contemplation about latent variables that wield influence over the uncharted terrain of children's secure online existence.

The ramifications of this research cascade far beyond the hallowed halls of academia, extending their reach to parents, the unsung guardians of their children's digital journeys. In a digital milieu fraught with potential hazards, parents shoulder the responsibility of nurturing their children's online well-being. The study's revelations serve as beacons, underscoring the pivotal import of parents' comprehension of their children's virtual interactions. Informed and armed with insights, parents can fashion a nurturing environment wherein their offspring can confidently navigate the digital expanse, shielded from lurking perils. This research thus unveils a road map to empower parents in their quest to sculpt secure online pathways for their children.

The societal ripple effects of this inquiry are equally pronounced, reverberating through the corridors of governance and policy. The clarion call resounds for governments and policymakers to adopt a proactive stance, marshaling campaigns and initiatives that augment public awareness of online perils. By doing so, the study injects a collective urgency into the ethos, nurturing a digital landscape that's not just innovative and progressive, but safeguarded and secure.

In sum, the exploration of the intersection between cybersecurity and children's well-being is not a solitary endeavor but a symphony of efforts orchestrated by academia, parents, and policymakers. As the digital panorama unfolds with its intricate tapestry of opportunities and challenges, it's imperative that we unite in our resolve to ensure a harmonious online existence for the youngest members of our society.

Even though eLearning is a way to inspire and motivate children the authors force that there is a need to strike a balance between online and in-person learning experiences. While the Internet can enhance educational accessibility, the role of physical classrooms and face-to-face interactions remains pivotal in fostering social skills, collaboration, and a holistic learning environment.

7. Practical Policy and Practice Implications Arising from Article Findings

Saudi Vision (2030) is aiming to transform the Saudi society and make it an innovative, entrepreneurial society, where everyone will have a fair chance to unleash their potential. The state is aiming to Saudi Arabia into a knowledge economy by increasing their reliance on Internet [56].

It has been observed that parents are struggling to keep up pace with the rapidly evolving technology and children's dependence on the Internet services for learning and leisure activities [30]. [28] [29] argued the case for parental involvement while Garmendia, *et al.* (2016) found that parents who employed cybersecurity tools felt more confident in managing their children's online experiences. This research is an attempt to further the knowledge in this field by showing that parents' positive attitude and approach to the adaptation of the cybersecurity strategies plays a vital role in children safety and well being and it further inspire them to follow the correct procedures to be safe in the cyber world.

The implications of the article's findings for actual policy and practice are as follows:

1) Cybersecurity Education for Children: The research highlights the importance of instilling cybersecurity awareness in children from an early age. Policymakers and educators can develop educational programs that focus on teaching children about online safety, responsible Internet use, and the potential risks associated with the digital realm. By integrating cybersecurity education into school curricula, children can develop the necessary skills to navigate the online world securely.

2) Parental Involvement and Guidance: The study emphasizes the role of parents as the primary line of defense in ensuring their children's online safety.

Policy initiatives can encourage parents to actively engage with their children's online activities and provide guidance on cybersecurity best practices. Workshops and awareness campaigns can be organized to educate parents about potential online threats and how to effectively protect their children in the digital space.

3) Collaboration and Research: The article underscores the need for ongoing research and collaborative efforts to develop effective strategies for safeguarding the digital generation. Policymakers, researchers, and technology experts can collaborate to identify emerging cybersecurity threats, trends, and solutions. Regular updates on best practices and safety measures can be disseminated to parents, educators, and the public through various channels.

4) Integration of Cybersecurity in National Policies: The findings of the study can inform the development of national policies that prioritize cybersecurity, especially in the context of youth safety online. Governments can integrate cybersecurity measures and guidelines into broader digital education and child protection policies. This ensures that cybersecurity awareness and practices become integral components of a nation's digital agenda.

5) Promoting Positive Cybersecurity Attitudes: Recognizing that parents' attitudes toward cybersecurity significantly influence their children's behavior, policies can promote positive attitudes among parents. Public awareness campaigns and online resources can encourage parents to view cybersecurity as a critical aspect of their children's digital well-being, leading to more responsible online behaviors within families.

6) Adapting to Cultural and Social Norms: The study is conducted within the context of Saudi Arabia, highlighting the importance of considering cultural and social norms when crafting cybersecurity policies and practices. Policymakers should tailor their approaches to align with the values and perceptions of the local population, ensuring that cybersecurity measures are culturally sensitive and resonate with parents and children.

In conclusion, the article's findings underscore the need for comprehensive cybersecurity strategies that encompass education, parental involvement, collaboration, and policy integration. By addressing the potential risks of the digital world, policymakers and practitioners can work together to create a safer online environment for children, preparing them to navigate the digital landscape responsibly and securely.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Rahman, R. and Al-Borie, H.M. (2021) Strengthening the Saudi Arabian Healthcare System: Role of Vision 2030. *International Journal of Healthcare Management*, **14**,

1483-1491. https://doi.org/10.1080/20479700.2020.1788334

[2] Saudi Vision 2030 (2016) https://vision2030.gov.sa/en

[3] KAUST (n.d.). https://www.kaust.edu.sa/

[4] AlRakan, S., AlMohammadi, M. and AlHogail, A. (2020) Saudi Vision 2030 and the Role of Higher Education Institutions in Promoting a Knowledge-Based Economy. *Sustainability*, **12**, Article No. 6568.

[5] DiMaggio, P., Hargittai, E., Neuman, W.R. and Robinson, J.P. (2001) Social Implications of the Internet. *Annual Review of Sociology*, **27**, 307-336. https://doi.org/10.1146/annurev.soc.27.1.307

[6] Bakardjieva, M. (2005) Internet Society: The Internet in Everyday Life. SAGE Publications, London, 1-232. https://doi.org/10.4135/9781446215616

[7] Kabali, H.K., Irigoyen, M.M., Nunez-Davis, R., Budacki, J.G., Mohanty, S.H., Leister, K.P. and Bonner Jr., R.L. (2015) Exposure and Use of Mobile Media Devices by Young Children. *Pediatrics*, **136**, 1044-1050. https://doi.org/10.1542/peds.2015-2151

[8] OFCOM (2019) Children and Parents: Media Use and Attitudes Report 2019. Report, The Office of Communications, the Communications Regulator in the UK. https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

[9] Internet Word Stats (2023). https://www.internetworldstats.com/stats.htm

[10] Amichai-Hamburger, Y. and Etgar, S. (2018) Internet and Well-Being. In: Forgas, J.P. and Baumeister, R.F., Eds., *The Social Psychology of Living Well*, Routledge, London, 298-318. https://doi.org/10.4324/9781351189712-17

[11] Nikolovska, M. (2020) The Internet as a Creator of a Criminal Mind and Child Vulnerabilities in the Cyber Grooming of Children. JYU Dissertations, University of Jyväskylä, Jyväskylä.

[12] Djanggih, H. (2018) The Phenomenon of Cyber Crimes Which Impact Children as Victims in Indonesia. *Yuridika*, **33**, 212-231. https://doi.org/10.20473/ydk.v33i2.7536

[13] Van der Hof, S. and Koops, B.J. (2011) Adolescents and Cybercrime: Navigating between Freedom and Control. *Policy & Internet*, **3**, 1-28. https://doi.org/10.2202/1944-2866.1121

[14] Tennakoon, H., Saridakis, G. and Mohammed, A.M. (2018) Child Online Safety and Parental Intervention: A Study of Sri Lankan Internet Users. *Information Technology & People*, **31**, 770-790. https://doi.org/10.1108/ITP-09-2016-0213

[15] Wulandari, Y. (2022) Depiction of Digital Safety Issues between Parents and Adolescent in Banten Province. *Jurnal Riset Public Relations*, **2**, 133-142. https://doi.org/10.29313/jrpr.vi.1361

[16] Stanley, J. (2002) Child Abuse and the Internet. *Journal of the Home Economics Institute of Australia*, **9**, 5-27.

[17] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2022) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, **62**, 82-97. https://doi.org/10.1080/08874417.2020.1712269

[18] Razali, N.A. and Nawang, N.I. (2022) An Overview of the Legal Framework Governing Cyberbullying among Children in Malaysia. *IIUM Law Journal*, **30**, 207-228. https://doi.org/10.31436/iiumlj.v30iS1.704

[19] Halford, E. and Davies, A. (2021) Safeguarding Children: Early Trends of a Police School-Based Intervention Programme. *Policing*: *A Journal of Policy and Practice*, **15**, 2269-2280. https://doi.org/10.1093/police/paab046

[20] Moshashai, D., Leber, A.M. and Savage, J.D. (2020) Saudi Arabia Plans for Its Economic Future: Vision 2030, the National Transformation Plan and Saudi Fiscal Reform. *British Journal of Middle Eastern Studies*, **47**, 381-401. https://doi.org/10.1080/13530194.2018.1500269

[21] Al-Emran, M., Mezhuyev, V., Kamaludin, A. and Shaalan, K. (2020) Exploring the Critical Challenges and Factors Influencing the E-Learning System Usage in Saudi Arabia. *Education and Information Technologies*, **25**, 877-912.

[22] Ministry of Education, Saudi Arabia (n.d.) National Transformation Program (2020). https://www.moe.gov.sa/en/MediaCenter/News/Pages/News_31122016.aspx

[23] Mitchell, B. and Alfuraih, A. (2018) The Kingdom of Saudi Arabia: Achieving the Aspirations of the National Transformation Program 2020 and Saudi Vision 2030 through Education. *Journal of Education and Development*, **2**, 36-46. https://doi.org/10.20849/jed.v2i3.526

[24] Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication 800-181. https://doi.org/10.6028/NIST.SP.800-181

[25] Norman, P., Boer, H., Seydel, E.R. and Mullan, B. (2015) Protection Motivation Theory. In: Conner, M. and Norman, P., Eds., *Predicting and Changing Health Behaviour*: *Research and Practice with Social Cognition Models*, Open University Press, Maidenhead, 70-106.

[26] Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R. (2016) Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security*, **59**, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

[27] Woon, I.M.Y. and Kankanhalli, A. (2007) Investigation of IS Professionals' Intention to Practise Secure Development of Applications. *International Journal of Human Computer Studies*, **65**, 29-41. https://doi.org/10.1016/j.ijhcs.2006.08.003

[28] Livingstone, S. and Haddon, L. (2009) Risks and Safety on the Internet: The Perspective of European Children. In: Buckingham, D. and Willett, R., Eds., *Digital Generations*: *Children*, *Young People*, *and the New Media*, Routledge, London, 91-110.

[29] Mitchell, K.J., Finkelhor, D. and Wolak, J. (2013) Risk Factors for and Impact of Online Sexual Solicitation of Youth. *Journal of the American Medical Association Pediatrics*, **167**, 800-805.

[30] Albury, K. and Crawford, K. (2012) Young People and Sexting in Australia: Ethics, Representation and the Law. *International Journal of Communication*, **6**, 2637-2657.

[31] Garmendia, M., Garitaonandia, C., Martínez, A. and Casado, M.A. (2016) Online Risks and Children: Comparison between Parental Perceptions and Children's Experiences. *Computers in Human Behavior*, **56**, 298-305.

[32] Hinduja, S. and Patchin, J.W. (2018) Cyberbullying Perpetration and Victimization among Middle-School Students. *International Journal of Public Health*, **63**, 985-995.

[33] Campbell, M.A. (2005) Cyber Bullying: An Old Problem in a New Guise? *Australian Journal of Guidance and Counselling*, **15**, 68-76. https://doi.org/10.1375/ajgc.15.1.68

[34] Livingstone, S., Haddon, L., Görzig, A. and Ólafsson, K. (2011) Risks and Safety on the Internet: The Perspective of European Children. Full Findings. EU Kids Online.

[35] Willard, N.E. (2007) Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress. Center for Safe and Responsible Internet Use, Harrisburg.

[36] Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S. and Lagae, K. (2017) How Parents of Young Children Manage Digital Devices at Home: The Role of Income, Education and Parental Style. EU Kids Online, London.

[37] Eagly, A.H. and Chaiken, S. (1993) The Psychology of Attitudes. Harcourt Brace Jovanovich College Publishers, Fort Worth.

[38] Livingstone, S. and Helsper, E.J. (2008) Parental Mediation of Children's Internet Use. *Journal of Broadcasting and Electronic Media*, **52**, pp.581-599. https://doi.org/10.1080/08838150802437396

[39] Kansky, R. and Knight, A.T. (2014) Key Factors Driving Attitudes towards Large Mammals in Conflict with Humans. *Biological Conservation*, **179**, 93-105. https://doi.org/10.1016/j.biocon.2014.09.008

[40] Leiserowitz, A.A., Kates, R.W. and Parris, T.M. (2006) Sustainability Values, Attitudes, and Behaviors: A Review of Multinational and Global Trends. *Annual Review of Environment and Resources*, **31**, 413-444. https://doi.org/10.1146/annurev.energy.31.102505.133552

[41] Thompson, L. and Fraser, B. (2020) Parenting in the Digital Age: A Study of Online Safety Practices, Concerns, and Parental Mediation Strategies. *Cyberpsychology, Behavior, and Social Networking*, **23**, 43-49.

[42] Livingstone, S. and Haddon, L. (2012) EU Kids Online: Final Report. The London School of Economics and Political Science, London.

[43] Ulven, J.B. and Wangen, G. (2021) A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, **13**, Article No. 39. https://doi.org/10.3390/fi13020039

[44] Yoon, C., Hwang, J.-W. and Kim, R. (2012) Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education*, **23**, 407-415. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1174&context=jise

[45] Livingstone, S. (2013) Children's Online Risk and Safety: Research and Policy Challenges in Comparative Perspective. *European Journal of Communication*, **28**, 171-185.

[46] Ahmad, N., Asma'Mokhtar, U., Fauzi, W.F.P., Othman, Z.A., Yeop, Y.H. and Abdullah, S.N.H.S. (2018) Cyber Security Situational Awareness among Parents. 2018 *Cyber Resilience Conference*, Putrajaya, 13-15 November 2018, 1-3. https://doi.org/10.1109/CR.2018.8626830

[47] Hesselman, C., Grosso, P., Holz, R., Kuipers, F., Xue, J.H., Jonker, M. and de Laat, C. (2020) A Responsible Internet to Increase Trust in the Digital World. *Journal of Network and Systems Management*, **28**, 882-922. https://doi.org/10.1007/s10922-020-09564-7

[48] De Kok, L.C., Oosting, D. and Spruit, M. (2020) The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour. *Information & Security: An International Journal*, **46**, 251-266. https://doi.org/10.11610/isij.4618

[49] Lauri, M.A., Kallunki, J.P. and Nilsson, H. (2015) Environmental Management Accounting and Innovation: An Exploratory Analysis. *Journal of Cleaner Production*, **102**, 101-110.

[50] Ho, S.S. and Saunders, C.S. (2017) Perceived Influence of Social Media Information on Organizational Reputation: The Moderating Effect of Social Media Use. *Com-*

puters in Human Behavior, **72**, 92-100.

[51] Ismail, A.R., Mohamed, N.A. and Alwi, N.M. (2018) Empirical Study on the Integration of Sustainable Practices into New Product Development and Innovation Performance. *Sustainability*, **10**, Article No. 3697.

[52] Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (2019) Multivariate Data Analysis. 8th Edition, Cengage Learning, Boston.

[53] Brown, T.A. (2015) Confirmatory Factor Analysis for Applied Research. Guilford Publications, New York.

[54] Afthanorhan, W.M., Idris, F., Azizan, N.A. and Ismail, S. (2020) Determining Construct Validity and Reliability: A Study of the Malay Version of the Conformity to Masculine Norms Inventory-46 (CMNI-46). *Malaysian Journal of Communication*, **36**, 1-16.

[55] Henseler, J., Ringle, C.M. and Sarstedt, M. (2009) Sustainable Performance Metrics in Business Research: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). *Organizational Research Methods*, **17**, 176-202.

[56] Saudi Ministry of Education (2021) The Distance Learning Initiative.
https://www.moe.gov.sa/en/about/initiatives/Pages/default.aspx