Economic Affairs, Vol. 68, No. 04, pp. 1957-1967, December 2023
DOI: 10.46852/0424-2513.4.2023.7

AESSRA

Research Paper

An Investigation of the Relationship Between Parents' Socio-economic Standards and their Children's Online Safety; Perspective: Bangladesh

Rumel M.S. Rahman Pir*, Md. Forhad Rabbi and M. Jahirul Islam

Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh

*Corresponding author: rumelpir@student.sust.edu (**ORCID ID:** 0000-0003-2800-580X)

Received: 20-09-2023 **Revised:** 05-11-2023 **Accepted:** 30-11-2023

ABSTRACT

The field of child-computer interaction has garnered significant interest from researchers worldwide. Nevertheless, the discourse around the protection of children's digital safe, that includes privacy and security remains significantly underrepresented in both Bangladesh and the broader global south. In situations where a significant portion of senior and adult persons lack awareness regarding optimal strategies for effectively utilizing digital gadgets and tools, it is difficult to anticipate a higher level of proficiency among younger individuals. Privacy generally encompasses the capacity of individuals to exercise control over, get access to, and govern their personal data. In contrast, the security system serves to mitigate the risk of unauthorized access, data leakage, or cyber intrusions, therefore safeguarding the data from potential compromise. Previous studies have indicated that the responsibility for safeguarding the digital privacy and security of children lies with both parents and children themselves. Regrettably, a dearth of scholarly investigations exists within the domain, hindering the ability to systematically monitor and analyze the potential relationship between parental socioeconomic status and the privacy and safety of their offspring. This research aims to discover the correlation. This study employed semi-structured interviews with a sample of 48 parents and 42 children from diverse socioeconomic backgrounds, including high income, middle income, and low-income groups. The collected data were subjected to statistical analysis. The findings of this study indicate that children from high income families are more susceptible to online safety issues compared to their counterparts from low-income households. This vulnerability is attributed to factors such as the widespread availability of internet access and personal digital devices, greater purchasing power on online platforms, and a lack of parental monitoring. This study presents a limited number of recommendations for parents and children across various socioeconomic backgrounds in order to enhance the state of internet safety for children.

HIGHLIGHTS

- Children in Bangladesh are using devices with internet access on a regular basis. In addition, children's online security and privacy are being threatened by their actions.
- Owing to factors such as personal digital device ownership, internet accessibility, and parent-child communication gaps, children from higher socio-economic backgrounds are more likely to experience problems with online safety.
- It was found that if children could change their usage habits and act more responsibly online, their digital privacy and security circumstances would improve.
- Moreover, Parental supervision of their children's online activity needs to be strengthened. More time spent with their kids and open communication about their social circle, online activity, and other topics can potentially lead to improved safety measures.

Keywords: Children, Privacy, Security, Cyber Awareness, socio-economic status

How to cite this article: Rumel M.S. Rahman Pir, Forhad Md. R. and Jahirul Islam, M. (2023). An Investigation of the Relationship Between Parents' Socio-economic Standards and their Children's Online Safety; Perspective: Bangladesh. *Econ. Aff.*, **68**(04): 1957-1967.

Source of Support: None; **Conflict of Interest:** None

Typically, children are initially introduced to technology during the early phases of their development (Sivrikova *et al.* 2020). The individual's introduction to the internet may start throughout the early phases of their cognitive and physical growth, through the utilization of Internet of Things (IoT) devices like as sensors, monitors, wearables, and engagement with IoT toys, among other activities (Mertala, 2020). Children may find themselves in an environment where they are encompassed by intelligent equipment such as televisions, computerized personal assistants, and various other Internet of Things (IoT) devices that have the capability to continuously gather data on them (Manches *et al.* 2015). Hence, it would provide a significant challenge for youngsters to evade observation in the contemporary period. The internet, despite its numerous advantages, presents significant risks to children due to their frequent and often unintentional exposure to it (Pir *et al.* 2022). These gadgets have the potential to be utilized in a manner that is improper for contacting children, exposing them to information that is harmful, and in certain situations, causing both psychological and physical injury (Pir *et al.* 2022; Pir *et al.* 2023). In addition to these aforementioned risks, the societal inclination towards a pervasive period of monitoring has a profound impact on children's conceptions of liberty and detrimentally impinges upon their inherent entitlement to privacy (Livingstone *et al.* 2019). Similar to their interaction with adults, Internet of Things (IoT) gadgets gather data about children and send it via the internet, allowing service providers to store it indefinitely for diverse objectives. These gadgets, which are presently not included under the legislative framework designed to safeguard minors, have the potential to be outfitted with a multitude of sensors capable of capturing audio, conversations, geographical coordinates, and even visual content of anyone present in their proximity (Stoilova *et al.* 2020; Pir *et al.* 2022)

When investigating the domain of children's digital experiences, it is essential to acknowledge the interdependence of privacy and security. Nonetheless, it is essential to observe that these two categories are distinct (Andrews *et al.* 2020). Privacy generally refers to an individual's authority over, access to, and management of their personal data (Crepax *et al.* 2022). The purpose of privacy regulations is to protect the interests of minors by prohibiting the unauthorized disclosure of their personal information to unfamiliar third parties, unless the children or their parents provide express consent. Also effective are privacy safeguards for protecting the data of minors from unauthorized access or larceny (Ní Bhroin *et al.* 2022). In contrast, security refers to the mechanism used to protect data from unauthorized access, whether through an intrusion, a disclosure, or a cyber-attack. In addition, it is important to note that security measures play an essential role in ensuring the safety of minors in the digital domain (Ondrušková,& Pospíšil, 2023). In the event that the privacy and security of children in the digital domain are compromised, they may be subjected to cyberbullying, harassment, and threats, among other forms of online misconduct (Crepax *et al.* 2022; Ondrušková & Pospíšil, 2023). Several common privacy and security issues associated with juveniles include password hacking, password abuse, installing malware, phishing, and access to inappropriate information (Gür & Türel, 2022). Children's physical and mental health can be negatively affected by the invasion of their privacy in online environments. These effects may manifest in a variety of ways, including depression, tension, heightened anxiety, difficulties traversing social media platforms, sleep disturbances, and avoidance behaviors (Kumar *et al.* 2017). The prospective disclosure of an individual's personal information may have implications for their physical health. Parents and children's social security could be jeopardized if the cybercriminal were to obtain sensitive information. It has been documented that hackers have obtained the financial information of parents by exploiting their children's online perplexity (Chu *et al.* 2018). The exposure of children to inappropriate and adult content on the Internet could have profound and lasting effects on their cognitive development (Kumar *et al.* 2017; Pir *et al.* 2023).

The purpose of this study was to determine the relationship between the children's privacy and safety and their parents' socioeconomic status. Bangladesh's economy is a prominent market economy in development (Pomi *et al.* 2022). As the second largest economy in South Asia, Bangladesh's economy ranks 33rd in nominal terms and 25th in

terms of purchasing power parity (Park & Yeung, 2022). Agriculture, garment manufacturing, and the service sector are the most important economic sectors in Bangladesh (Nath, 2021). Therefore, there are various categories of families based on their financial independence. The categorization of households into those with a high income, a moderate income, and a low income was crucial and difficult for this study. We first attempted to define families of median income. Then, low-income families were defined as those with a lower income than middle-class families. High income families are, as expected, defined as those with a higher income than middle income families. The Asian Development Bank (ADB) classifies the inhabitants of South Asian countries such as Bangladesh who earn between $2 and $20 per day as middle class (Beedel, 2019) when viewed from an economic standpoint. Nonetheless, this report dates quite a while ago. Despite this, defining middle-income families in Bangladesh is difficult due to the fact that it depends on a variety of factors, such as the number of family members, the city in which the family resides, and other such factors (Hussein, 2017). Recent studies have shown, however, that families earning less than 30000 Bangladeshi taka (BDT) can be considered low-income, whereas middle-income families have an average monthly income between 30000 and 70000 BDT (Hussein, 2017; Beedel, 2019). In our study, we have divided households into three categories based on their total monthly income in Bangladeshi taka as of 2023, as determined by the aforementioned data. Table 1 displays the information.

Table 1: Family categories based on earnings

Family Category	Monthly Earning (BDT)
Low Income	Below 30000
Middle Income	30000 to 70000
High Income	Above 70000

After dividing families in three different groups: low income, middle income and high income, the authors conducted semi-structured interviews with 48 parents and 42 children from all three socioeconomic standards and have analyzed that, the children of high income families and middle income families are more at risk of online privacy and security violations compared to the children of low income families due to availability of internet access, higher ownership of digital gadgets, better purchase power through internet, internal family environment and higher uses of social media. We compared the findings from the parents and children's interviewees and the results were justified. Finally, we have provided some recommendations both for the parents and children so that the online safety of the children can be improved for all types of socioeconomic standards.

BACKGROUND STUDY

Childhood and adolescence are junctures characterized by developmental milestones and first encounters with risky behaviors. Due to their limited cognitive capacity to fully comprehend the causal relationship between their actions and the ensuing consequences, adolescents and young adults are especially susceptible to harm (Arendt *et al.* 2021). Moreover, the pervasive presence of digital technology has a growing impact on children's daily existence, manifesting itself in both domestic and educational settings (Pir *et al.* 2023). People devote a considerable amount of time to a variety of electronic devices, including mobile phones, tablets, laptops, and technologically advanced games (Livingstone *et al.* 2019). In the aftermath of the COVID-19 pandemic, there has been a significant increase in the duration of digital technology use among young people (Limone & Toto, 2021). Youth today use digital devices for a wide variety of activities, including social interactions, gaming, interpersonal communication, and educational endeavors (Domoff *et al.* 2019). The increase in user population has been accompanied by a rise in the number of parents who are concerned about their children's online safety and privacy (Livingstone *et al.* 2019; Domoff *et al.* 2019). The use of digital technology raises a wide variety of privacy and security concerns. These concerns include both abstract anxieties, such as surveillance and identity theft, and more practical constraints, such as avoiding humiliation and maintaining schedule control (Duan *et al.* 2020). This issue has been exacerbated by the increasing global prevalence of internet utilization and the extensive popularity of social media platforms among the younger demographic (Drouin *et al.* 2020). Consequently, a substantial proportion of children and adolescents experience online victimization of various varieties at some point in their lives. Online victimization can

manifest in a variety of ways, including cyber abuse, cyberbullying, threats, and other similar forms of online malfeasance (Razon & Ahmad, 2017; Pir *et al.* 2023). Numerous negative effects of the digital domain on the well-being of the younger generation include invasions of their personal privacy and the emergence of psychiatric disorders (Girela-Serrano *et al.* 2022). Despite the widespread belief among parents that addressing this issue is unimportant, empirical evidence from researchers demonstrates that parents can play a crucial role in protecting and enhancing the privacy and security of their children within the digital domain (Akter *et al.* 2022). Nonetheless, it is essential to recognize that parents cannot assume sole responsibility for their children's well-being if the children fail to assert themselves and report instances of misconduct (Pir *et al.* 2023). When confronted with the task of maintaining self-discipline in unfamiliar situations, infants and adolescents tend to perform less well than adults, resulting in sub-optimal outcomes. This is especially true when confronted with peer pressure and intense personal motivation. The propensity of adolescents to reject conventional risk treatments can be attributed to impulsivity, a desire for delight and stimulation, and other individual differences (Fox & Hoy, 2019; Gür & Türel, 2022).

Researchers in the field of Human-Computer Interaction (HCI) view the investigation of children's understanding of data sharing and privacy concepts in the context of the Internet as a crucial issue. Consequently, they frequently conduct research on this subject (Hartikainen *et al.* 2019). Using the visual programming language Scratch, children as young as 8 years old were able to comprehend the privacy implications associated with the public accessibility and searchability of data, according to a study (Haber, 2020). It has been determined, for instance, that the process of collecting and storing data is accompanied by numerous privacy concerns. In addition, the examination of data requires a critical mindset and the ability to effectively interpret it. In addition, it is essential to recognize that data includes underlying assumptions and concealed judgments. Based on the findings of a previous study (Kumar *et al.* 2019), it was determined that children between the ages of 6 and 10 were aware that internet-connected devices could record and rebroadcast their conversations. However, they did not establish the correlation that a third party could potentially eavesdrop on their online conversations. Based on the findings of a distinct study, it was determined that children between the ages of five and eleven possessed a fundamental comprehension of the concept that certain information may be sensitive and should only be disclosed to dependable individuals (Desimpelaere *et al.* 2020). In contrast, young adults demonstrated a significant inability to fathom complex issues, such as the influence of communication platforms on individuals' privacy and security levels (Hartikainen *et al.* 2019; Haber, 2020). In conclusion, our study indicates that a subset of younger children have a fundamental comprehension of online privacy and security. Nonetheless, it is evident that these younger children would benefit from increased adult supervision to protect their privacy and safety from potential hazards (Tyagi *et al.* 2020).

Commonly, the hazards associated with Internet use fall into two categories: content threats and contact threats (Pir *et al.* 2023). Additionally, it is essential to consider the incorporation of both physical and digital threats within the category (Kumar *et al.* 2017). The term "content threats" refers to numerous types of inappropriate material that may be harmful to minors. These include commercial spam and targeted emails/ads that view children as active customers, in addition to adult/abusive content such as pornography, violence, pro-anorexia, and drug-related material (Crepax *et al.* 2022). Contact threats include multiple forms of detrimental behavior, such as grooming, adultery, cyberbullying, cyberstalking, and invasion of privacy (Andrews *et al.* 2020). Grooming refers to the process by which an adult cultivates an emotional bond with a child in order to engage in sexual assault. Sexting is the act of sending sexually explicit messages via text or messaging platforms. Cyberbullying and cyberstalking involve the use of technology to torment another individual. Threatening behaviors include instances in which a minor engages in actions that are either illegal or prohibited, such as engaging in unauthorized file sharing or engaging in harassing behaviors (Crepax *et al.* 2022). Computer and internet hazards include a variety of information security risks, such as malware, which is software designed to damage computer systems, obtain illicit access, or steal sensitive data. Moreover, phishing is a deceptive

practice designed to induce users to divulge private information by impersonating reputable organizations. Other hazards include the theft or loss of data, the theft or hacking of passwords, and the issue of internet addiction (Ní Bhroin *et al.* 2022; Crepax *et al.* 2022). While certain child control applications and child safety settings can restrict children's access to inappropriate content on the internet, they cannot assure children's complete privacy and security in the current digital world (Park & Yeung, 2022).

METHODS

Our study had three objectives: (1) to determine the relationship between the socioeconomic status of families and the online safety of children; (2) to identify significant socioeconomic factors that make children's lives unsafe online; and (3) to recommend ways to improve online safety for children of all socioeconomic backgrounds. In order to accomplish the stated objectives, a qualitative field study was undertaken in a city in Bangladesh, named Sylhet. Semi-structured interviews were conducted with a total of 48 parents and 42 children. The parents and the children belong to different socioeconomic background: low income, middle income and high income.

Semi-structured Interviews

Semi-structured interviews were conducted with participants throughout the period of February to August 2023. All of the authors were native to Bangladesh, having been born and raised there. They possessed fluency in the local language, Bengali, and exhibited a deep understanding of the indigenous culture and customs. Our study started by employing convenience sampling to recruit parents' participants. Initially, a cohort of 8 parents were recruited via the social network of the authors. The initial cohort of 8 individuals subsequently facilitated the recruitment of an additional 40 participants using the snowball sampling method, ultimately achieving theoretical saturation. A total of 48 parents were recruited for the study.

For recruiting children, the authors visited 6 different schools in Sylhet, Bangladesh and interviewed the children during their class breaks and tiffin periods. 6 schools were chosen randomly, however 2 of these were English Medium schools, 3 were Bangla Medium and 1 Madrasa. We took help of the teachers from those schools while choosing participants for the interviews. In all these interviews, at least one teacher was present beside the student.

The act of participating in the study was done on a voluntary basis. The duration of the interviews ranged from around 15 to 25 minutes, and they were performed in a one-on-one format. The interviews were done exclusively in the Bengali language, either at the participants' houses (parents) or at their academic campus (children). The interviews were semi-structured and guided by a list of topics. During the interviews of the parents, the researchers gathered demographic data, professional information, monthly average income, their views and actions on their children's online privacy and security etc. The children were asked about their parent's profession, online uses, privacy and security practices, device sharing habits, gadget ownership, online shopping practices etc. Additionally, we inquired about the child participants' parental income with their teachers separately. We solicit comments from both the parents and the children regarding their strategies to enhance the safety of the digital environment for children.

(a) Participant Characteristics

Our 48 parent participants (40 males and 8 females) came from different socioeconomic background and ranged in age from 30 to 45 years (average = 40). Participants possessed different academic backgrounds. Out of 48 parents, 22 were graduates or post graduates. Among others, 12 completed Secondary School Certificate (SSC) exams and remaining 14 do not have good academic background (below SSC). As per the criteria of this study, 18 parents were classified as low-income parents, 22 were classified as middle-income group and only 8 parents were identified as high-income group. Their profession also varies greatly. The professions of these parents are widely different; there were professor, doctor, engineer, banker, police officer, small shop owner and businessman, office clerk, bus driver, ricksha puller, home maker, day laborer who were amongst the participants.

Among the 42 children, as per our set criteria, 15 were identified who belong to low-income family while 19 children were identified from middle

income family. Remaining 8 children were classified to belong from high income families. This is shown in the Table 2. The age range of the children interviewees are from 8 to 14 years (average = 11).

Table 2: Children from different background

Family Category	Number of Participants
Low Income	15
Middle Income	19
High Income	8
Total	**42**

(b) Data Collection and Analysis

The data collected yielded a cumulative duration of 30 hours of audio-recorded interview material and an extensive volume of field notes spanning hundreds of pages. The interviews were transcribed and translated into English by two team members who are proficient in Bengali as their first language. Subsequently, an inductive analysis was conducted on the interview transcripts. The initial step involved many iterations of carefully reviewing the transcripts, enabling the identification of codes that emerged from the dataset. The codes were iteratively improved prior to grouping them into high-level themes that encapsulate our significant findings, as detailed in the subsequent sections. Statistical analysis was conducted when deemed essential. The final codes and themes were agreed upon by all members of the team. The findings from the parents' participants and the finding from the children's participants were then carefully compared to justify the analysis.

FINDINGS

After thorough analysis on the interview data, there were few significant findings regarding the correlations between the socioeconomic standards of the children and parents with the privacy and security of the children and adolescents. The findings are listed below:

(a) Time spent online

Numerous prior studies indicate a positive correlation between the duration of children's internet usage and their susceptibility to online risks (Kardefelt-Winther *et al.* 2020; Jeong *et al.* 2021). Based on the testimonies provided by the interview participants, including both parents and children, it became evident that children belonging to higher income and middle-income households dedicate much more time to internet usage in comparison to children from lower income homes. Based on the data provided by the parents, it was observed that children belonging to better income families tend to spend an average of 7 hours per day on the internet, whilst children from lower income families often spend just 2 hours per day engaged in online activities. The increased amount of time spent on the internet has led to a higher likelihood of online safety hazards for children from higher income households and medium income families, compared to children from lower income families.

(b) Accessibility of internet

Our investigation uncovered a disparity in the accessibility to the internet among youngsters. Children from better income socioeconomic backgrounds have greater accessibility to the internet compared to their counterparts from lower income family groups. The presence of internet connectivity poses potential risks to children from high and middle-income backgrounds, in contrast to children from lower-income backgrounds. The Table 3 displays the extent to which children have access to the internet based on data obtained from interviews.

Table 3: Children with internet access

Family Category	Percentage (%)
Low Income	20%
Middle Income	68%
High Income	100%

Previous scholars have also engaged in discourse about the existence of a favorable association between children's internet accessibility and their vulnerability to online platforms. When children are provided with convenient and unrestricted access to the internet, they tend to engage in more frequent communication with others beyond their immediate environment (Stoilova *et al.* 2021). As an illustration, individuals engage in online gaming activities and interact with unfamiliar individuals with whom they engage in chat-based communication. Several kid participants said that they engage in the practice of downloading applications from the internet

without the knowledge or awareness of their parents. Individuals access online content that may not be suitable for children. Due to the accessibility of internet connection, children from higher income and medium income households are at a greater risk of safety breaches compared to children from lower income families.

(c) Ownership of digital gadgets

The practice of sharing digital gadgets is prevalent in nations such as Bangladesh (Ahmed *et al.* 2019). However, this does not align with the circumstances experienced by numerous affluent households. The results of our study indicate that children from better income households typically possess personal digital devices such as laptops, PCs, and cellphones. Even within middle-income households, a significant number of children possess personal digital devices. However, the situation contrasts significantly when considering children from lower income households. According to the responses obtained during the interview, it was reported by parents belonging to a lower income demographic that none of their children own personal digital devices. All of the instruments utilized are communal in nature which is serving as a means of safeguarding their personal security. Children frequently utilize their personal digital devices for activities that are deemed unsafe (Kumar *et al.* 2019). Previous studies have indicated that parental monitoring plays a crucial role in protecting the digital privacy and security of children (Chu *et al.* 2018). The ability to effectively supervise children's online activities becomes challenging when they have their own personal devices (Pir *et al.* 2023). Consequently, children from lower-income households are somewhat safer online compared to their counterparts from wealthier and middle-income homes.

(d) Online shopping habbits

Based on the insights gathered from our interview participants, it has been observed that youngsters hailing from low-income homes exhibit minimal engagement in online buying activities. However, a significant proportion, almost 30%, of youngsters from middle-income homes have developed a familiarity with engaging in online buying activities. In contrast, internet buying is widely prevalent among youngsters from affluent households. During the interview, participants from affluent households reported that their parents had granted them access to credit cards, enabling them to make online purchases or order food at their discretion. The absence of parental monitoring while online purchasing poses potential risks to children, so compromising their overall online safety. In contrast, children from low-income households have a somewhat lower level of vulnerability compared to their counterparts from middle- and high-income families, mostly stemming from their limited exposure to and limited financial means for engaging in online purchasing activities.

(e) Parents-children relationship

Previous studies have indicated that the interaction between children and their parents is of utmost importance in establishing a secure internet environment for young people. This relationship can be broadly characterized as the extent to which children engage in discussions with their parents regarding their online environment, including whether they disclose instances of encountering online hazards such as cyberbullying or threats (Ktoridou *et al.* 2012). Additionally, it encompasses whether parents provide their children with education on how to safeguard themselves while using the internet, among other factors (Ktoridou *et al.* 2012; Livingstone *et al.* 2017). This study reveals that the level of closeness in the children-parents connection regarding discussions about online life inside the family is much higher in low-income and middle-income households as opposed to high-income families. Research has indicated that children hailing from high-income households typically possess personal digital gadgets and have access to individual living spaces inside their homes. Conversely, these resources are sometimes financially unattainable for low-income families and a significant portion of middle-income families. Low-income households typically engage in the practice of room sharing within their residences, in addition to sharing digital equipment between family members. Therefore, children originating from these households tend to develop stronger bonds with their parents and engage in more frequent conversations on their digital environment, including potential risks and dangers,

with their parents. Therefore, youngsters hailing from economically disadvantaged backgrounds inherently take measures to enhance their safety.

(f) Social media uses

According to our study, children from high-income and middle-income households exhibit more frequent utilization of social media platforms such as Facebook, Twitter, Messenger, WhatsApp, and similar platforms, in contrast to children from low-income homes. According to the findings derived from interviews conducted with children, it was observed that children belonging to higher income households tend to utilize social media platforms more often. These children engage in activities such as regular talking, photo sharing, and divulging personal information, hence becoming themselves susceptible to online dangers (Hamm *et al.* 2015). According to our research, children from low-income homes exhibit infrequent usage of social media platforms, hence experiencing enhanced safety within the online milieu.

DISCUSSION

The advent of the Internet, mobile devices, and other electronic media has significantly expanded the accessibility of knowledge, culture, communication, and enjoyment for children and young people, surpassing previous levels that were inconceivable until recently (Nath, 2021). However, it is important to note that some of their remarkable benefits are accompanied with inherent hazards (Hussein, 2017; Nath, 2021). The Internet and related technologies have made it simpler to produce and disseminate violent pictures of children, and they offer major new possibilities for abusers to reach and interact with children and teenagers online. It was discovered that kids' digital privacy and security situations would improve if they could alter their usage patterns and behave more responsibly online (Hamm *et al.* 2015).

Research has indicated that parental involvement plays a crucial role in enhancing children's internet safety (Fox & Hoy, 2019). The participants in the interview also made note of a limited number of parental obligations. It is of utmost importance for persons responsible for the care of children, such as parents and teachers, to establish a more congenial rapport with them about their involvement in digital activities. It is recommended to foster a culture of open communication between minors and adults with regards to their internet activities, so enabling them to actively participate in dialogues pertaining to their daily encounters. In addition, it is imperative to foster an environment where children are motivated to expeditiously notify responsible adults of any occurrences of threats or harassment (Haleem *et al.* 2022). Moreover, it is crucial to offer young folks suitable educational opportunities to augment their comprehension of the possible hazards associated with exchanging passwords with classmates and other individuals. Parents possess the capacity to set passwords for their offspring and direct them to uphold the principle of secrecy with regards to this data [40]. Moreover, it is recommended that parents actively participate in open dialogues on their children's online connections, with the objective of minimizing or eliminating the presence of unknown individuals in their online social circles. It is crucial for parents and educators to aggressively advocate for the practice of abstaining from disclosing personal information, such as images, to unfamiliar persons within the realm of online communication or social media platforms. Furthermore, it is recommended that parents exert control or oversight over their children's downloading activities and online transactions, particularly in instances where such actions are carried out without parental agreement. In conclusion, it is crucial for parents and educators to place utmost importance on delivering comprehensive education on online privacy and safety to children. Numerous studies have provided evidence indicating that adolescents who possess sufficient knowledge regarding internet safety are much less susceptible to encountering cyber threats (Arendt *et al.* 2019; Park & Yeung, 2022).

The authors of this paper assert that there is a notable correlation between the internet safety of children and the socioeconomic context in which they are situated. As previously mentioned, the present study involved the implementation of semi-structured interviews with a total of 48 parents and 42 children, who were selected from three distinct socioeconomic categories. These three categories can be categorized as low-income, middle-income, and high-income based on the average monthly income of the parents. After conducting a comprehensive investigation, it was shown that youngsters

hailing from high-income and middle-income households exhibit a much higher susceptibility to online dangers and hazards as compared to their counterparts from low-income homes. Research has revealed that children from higher socioeconomic backgrounds are more vulnerable to risks associated with internet usage due to their lifestyle and online behavior patterns. These practices encompass a range of behaviors, including but not limited to increased time spent online, widespread availability of internet access, personal ownership of various digital devices, excessive engagement in online shopping, interpersonal dynamics between parents and children, and a heightened reliance on social media platforms. The limited access and affordability of digital devices and internet among children from lower income families contribute to their infrequent usage. However, this circumstance fosters a stronger bond between these children and their parents, resulting in enhanced safety within digital platforms.

RECOMMENDATIONS

In light of the aforementioned scenario, the authors have formulated many proposals aimed at enhancing online safety for children across all socioeconomic strata, with a particular focus on Bangladesh. The following items are:

1. There is a need for enhanced parental surveillance of children's internet activity. Enhanced safety measures can potentially be achieved if parents allocate additional time to their children and engage in open discussions on their social circle, online activities, and related matters. Furthermore, fostering an environment where children feel comfortable freely discussing any challenges encountered online with their parents can contribute to improved safety outcomes.
2. Given the inherent challenges faced by parents in completely disconnecting their children from the internet, it is advisable to establish a designated timeframe during which children are allowed to use the internet.
3. Unless it is absolutely necessary, it is not advisable to grant youngsters ownership of digital gadgets. In the initial stages, it is advisable for youngsters to utilize shared devices when accessing the internet, as this can enhance safety measures.
4. It is imperative that parental supervision be maintained while allowing children to make internet purchases. The aforementioned regulation should also be enforced in the context of downloading applications and viewing objectionable material on the internet.
5. It is advisable to restrict children's unfettered access to social media sites. It is not just the responsibility of parents to guarantee the understanding of privacy and security problems associated with the use of social media; children should also be knowledgeable in this respect.
6. Ultimately, it is insufficient for parents and children to alone bear the responsibility of safeguarding children in the digital realm. Ensuring a safer online environment for children necessitates the collaborative engagement of several stakeholders, including the government, regulatory agencies, educators, and kid application developers. Each of these entities must fulfill their respective responsibilities effectively. It is imperative to implement rigorous and consistent training programs for all relevant parties.

LIMITATIONS

There are some limitations inherent in this study. The parents who took part in the interview were selected using a combination of random selection and snowball sampling techniques. All of them are included on the list of primary and secondary contacts for the youngsters. Furthermore, the students were questioned within the school premises during their designated class breaks or during their allocated tiffin intervals. Consequently, they were compelled to respond to the questions hastily, without giving much consideration to their answers. Furthermore, it is important to note that all of the participants involved in the interviews are individuals residing in metropolitan regions. This study fails to include the perspectives and experiences of parents and children residing in rural regions.

CONCLUSION

The topic of internet safety for children is widely debated in contemporary society. Nevertheless, scholars continue to explore strategies aimed at enhancing the online safety of youngsters throughout their internet usage. The matter of children's internet safety in nations of the global south, such as Bangladesh, is of significant importance and cannot be disregarded. This study has investigated the influence of socioeconomic factors on the internet safety, privacy, and security of children. According to our research findings, youngsters hailing from financially stable households exhibit a higher susceptibility to online privacy and security breaches in comparison to their counterparts from disadvantaged backgrounds. The children from financially fortunate homes face increased dangers due to factors such as more internet accessibility, higher ownership of digital devices, and enhanced online purchasing power. By adhering to the guidelines outlined in this article, it is possible to enhance kid safety in the online environment. This work also provides an opportunity for future research to explore the dynamics between parents and children from diverse socioeconomic backgrounds in rural places. The scope of this research might potentially be expanded to present a conceptual framework aimed at safeguarding the online privacy and security of children in Bangladesh.

REFERENCES

Ahmed, S.I., Haque, M.R., Haider, I., Chen, J. and Dell, N. 2019. "Everyone Has Some Personal Stuff" Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).

Akter, M., Godfrey, A.J., Kropczynski, J., Lipford, H.R. and Wisniewski, P.J. 2022. From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals? *Proceedings of the ACM on Human-Computer Interaction*, **6**(CSCW1): 1-28.

Andrews, J.C., Walker, K.L. and Kees, J. 2020. Children and online privacy protection: Empowerment from cognitive defense strategies. *J. of Public Policy & Market.*, **39**(2): 205-219.

Arendt, F., Scherr, S. and Romer, D. 2019. Effects of exposure to self-harm on social media: Evidence from a two-wave panel study among young adults. *New Media & Society*, **21**(11-12): 2422-2442.

Beedell, A. 2019. *Negotiating Development: a psychosocial study of Bangladeshi development workers* (Doctoral dissertation, University of East London).

Chu, G., Apthorpe, N. and Feamster, N. 2018. Security and privacy analyses of internet of things children's toys. *IEEE Internet of Things J.*, **6**(1): 978-985

Crepax, T., Muntés-Mulero, V., Martinez, J. and Ruiz, A. 2022. Information technologies exposing children to privacy risks: Domains and children-specific technical controls. *Computer Standards & Interfaces*, **82**: 103624.

Desimpelaere, L., Hudders, L. and Van de Sompel, D. 2020. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, **110**: 106382.

Domoff, S.E., Radesky, J.S., Harrison, K., Riley, H., Lumeng, J.C. and Miller, A.L. 2019. A naturalistic study of child and family screen media and mobile device use. *J. of Child and Family Stud.*, **28**: 401-410.

Drouin, M., McDaniel, B.T., Pater, J. and Toscos, T. 2020. How parents and their children used social media and technology at the beginning of the COVID-19 pandemic and associations with anxiety. *Cyberpsychology, Behavior, and Social Networking*, **23**(11): 727-736.

Duan, L., Shao, X., Wang, Y., Huang, Y., Miao, J., Yang, X. and Zhu, G. 2020. An investigation of mental health status of children and adolescents in china during the outbreak of COVID-19. *J. of Affective Disorders*, **275**: 112-118.

Fox, A.K. and Hoy, M.G. 2019. Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers. *J. of Public Policy & Market.*, **38**(4): 414-432.

Girela-Serrano, B.M., Spiers, A.D., Ruotong, L., Gangadia, S., Toledano, M.B. and Di Simplicio, M. 2022. Impact of mobile phones and wireless devices use on children and adolescents' mental health: a systematic review. *Eu. Child & Adolescent Psychiatry*, pp. 1-31.

Gür, D. and Türel, Y.K. 2022. Parenting in the digital age: Attitudes, controls and limitations regarding children's use of ICT. *Computers & Edu.*, **183**: 104504.

Haber, E. 2020. The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World. *U. Ill. L. Rev.*, 1209.

Haleem, A., Javaid, M., Qadri, M.A. and Suman, R. 2022. Understanding the role of digital technologies in education: A review. *Sustainable Operations and Computers*, **3**: 275-285.

Hamm, M.P., Newton, A.S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P. ... and Hartling, L. 2015. Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. *JAMA Pediatrics*, **169**(8): 770-777.

Hartikainen, H., Iivari, N. and Kinnula, M. 2019. Children's design recommendations for online safety education. *Int. J. of Child-Computer Interaction*, **22**: 100146.

Hussein, N. 2017. Negotiating middle-class respectable femininity: Bangladeshi women and their families. *South Asia Multidisciplinary Academic J.*, **16**.

Kardefelt-Winther, D., Rees, G. and Livingstone, S. 2020. Contextualising the link between adolescents' use of digital technology and their mental health: A multi-country study of time spent online and life satisfaction. *J. of Child Psychology and Psychiatry*, **61**(8): 875-889.

Jeong, H., Yim, H.W., Lee, S.Y., Lee, H.K., Potenza, M.N. and Lee, H. 2021. Factors associated with severity, incidence or persistence of internet gaming disorder in children and adolescents: a 2-year longitudinal study. *Addiction*, **116**(7): 1828-1838.

Kumar, P., Naik, S.M., Devkar, U.R., Chetty, M., Clegg, T.L. and Vitak, J. 2017. 'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*, **1**(CSCW): 1-21.

Kumar, P.C., Chetty, M., Clegg, T.L. and Vitak, J. 2019. Privacy and security considerations for digital technology use in elementary schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).

Ktoridou, D., Eteokleous, N. and Zahariadou, A. 2012. Exploring parents' and children's awareness on internet threats in relation to internet safety. *Campus-wide Information Systems*, **29**(3): 133-143.

Limone, P. and Toto, G.A. 2021. Psychological and emotional effects of Digital Technology on Children in Covid-19 Pandemic. *Brain Sciences*, **11**(9): 1126.

Livingstone, S., Ólafsson, K., Helsper, E.J., Lupiáñez-Villanueva, F., Veltri, G.A. and Folkvord, F. 2017. Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *J. of Communication*, **67**(1): 82-105.

Livingstone, S., Stoilova, M. and Nandagiri, R. 2019. Children's data and privacy online: growing up in a digital age: an evidence review.

Manches, A., Duncan, P., Plowman, L. and Sabeti, S. 2015. Three questions about the Internet of things and children. *TechTrends*, **59**: 76-83.

Mertala, P. 2020. Young children's perceptions of ubiquitous computing and the Internet of Things. *British J. of Edu. Technol.*, **51**(1): 84-102.

Nath, N.C. 2021. Manufacturing sector of Bangladesh-growth, structure and strategies for future development. In *Bienn Conf "Global Econ. Vis* (pp. 1-43).

Ní Bhroin, N., Dinh, T., Thiel, K., Lampert, C., Staksrud, E. and Ólafsson, K. 2022. The privacy paradox by proxy: Considering predictors of sharenting. *Media and Communication*, **10**(1): 371-383.

Ondrušková, D. and Pospíšil, R. 2023. The good practices for implementation of cyber security education for school children. *Contemporary Edu. Technol.*, **15**(3): ep435.

Park, C.Y. and Yeung, B. 2022. An Integrated and Smart Association of Southeast Asian Nations: Overcoming Adversities and Achieving Sustainable and Inclusive Growth. *Harnessing Digitalization for Sustainable Economic Development*, **283**.

Pomi, S.S., Sarkar, S.M. and Dhar, B.K. 2021. Human or physical capital, which influences sustainable economic growth most? A study on Bangladesh. *Canadian J. of Business and Information Stud.*, **3**(5): 101-108.

Pir, Rumel M., Forhad Rabbi, and M. Jahirul Islam. 2023. Digitally Mediated Parenting in Bangladesh: Reality, Dangers and Answers. In *2nd International Conference on Human-Centric Smart Computing (ICHCSC-2023).*

Pir, R.M.R., Rabbi, M.F. and Islam, M.J. 2023. Applying a machine learning model to forecast the risks to children's online privacy and security. In *2023 Int. Conference on Intelligent Systems, Advanced Computing and Communication (ISACC)* (pp. 1-8). IEEE.

Razon, A.A. and Ahmad, I. 2017. A Study on Current Trends of Income and its Impact on Affordability in Multi-Ownership Housing in Demra, Dhaka. *Int. J. of Sci. and Res.*, **6**(3): 2187-2192.

Sivrikova, N.V., Ptashko, T.G., Perebeynos, A.E., Chernikova, E.G., Gilyazeva, N.V. and Vasilyeva, V.S. 2020. Parental reports on digital devices use in infancy and early childhood. *Edu. and Information Technol.*, **25**: 3957-3973.

Stoilova, M., Livingstone, S. and Nandagiri, R. 2020. Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, **8**(4): 197-207.

Stoilova, M., Livingstone, S. and Khazbak, R. 2021. Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes.

Tyagi, A.K., Rekha, G. and Sreenath, N. 2020. Beyond the hype: Internet of things concepts, security and privacy concerns. In *Advances in Decision Sciences, Image Processing, Security and Computer Vision: Int. Conference on Emerging Trends in Engineering (ICETE), Vol. 1* (pp. 393-407). Springer International Publishing.