Mesopotamian journal of Cybersecurity
Vol.4,No.2, **pp**. 63–73
DOI: https://doi.org/10.58496/MJCS/2024/007; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Cybersecurity Awareness among Special Needs Students: The Role of Parental Control

Hapini Awang[1, *], Nur Suhaili Mansor[1], Mohamad Fadli Zolkipli[1], Sarkin Tudu Shehu Malami [2], Khuzairi Mohd Zaini[1], Yau Ti Dun[3]

[1]*Institute for Advanced and Smart Digital Opportunities, School of Computing, Universiti Utara Malaysia, Malaysia*

[2]*Department of Computer Science and Information Technology, Faculty of Science, Sokoto State University, Sokoto, Nigeria*

[3]*Trainocate (M) Sdn. Bhd., Kuala Lumpur, Malaysia*

ARTICLEINFO

Article History

Received 05 Apr 2024
Accepted 18 May 2024
Published 10 Jun 2024

Keywords

Cybersecurity
Internet
Social media
Parent
Special need student

ABSTRACT

The awareness of cybersecurity among special needs students is necessary to help them stay safe while using technology. Recently, a good amount of interest has been drawn toward understanding the concepts and awareness of cybersecurity, and institutions have made efforts to help introduce awareness campaigns to help students understand the concepts of cybersafety, particularly for special needs students. The prior literature has focused primarily on exploring students' preferences, readiness, and experiences with cybersecurity. However, little attention has been given to measuring the level of cybersecurity awareness among students with special needs. To bridge this knowledge gap, the present study conducted an online survey to analyse the level of cybersecurity awareness and parental control among secondary school students with special needs aged 13 to 19 years in Malaysia. The study revealed that special needs students have a moderate level of cybersecurity awareness, with no significant difference among genders or academic streams. However, age does play a role in the level of awareness. Students with better cybersecurity knowledge are more satisfied with their online activities. Educating and monitoring special needs students on cyberattacks, password management, and phishing is crucial. In addition, parental control was found to be reasonable for most parents of students with special needs. This study contributes new knowledge by emphasizing the importance of parental control as a moderating variable in explanatory studies. It also highlights the need for further research in this area to expand the understanding of the importance of cybersecurity and how it can be implemented in specific school environments.

1. INTRODUCTION

Cybersecurity protects computer systems, networks, programs, and data from digital attacks. It uses various technologies, processes, and practices to safeguard devices, information, and infrastructure from cyber threats [1]. With increasing reliance on the internet, it has become more critical than ever to educate people about potential cyber threats and vulnerabilities associated with these threats. Due to the COVID-19 pandemic and the resulting increase in internet usage, cybersecurity awareness has become a highly debated issue among researchers, practitioners, and policymakers [2], [3], [4], [5]. Accordingly, although online distance learning (ODL) has become more prevalent in the educational context, offering convenience and promoting educational equality [6], there are risks associated with the heavy use of the internet among school students, particularly those who are still mentally immature [7]. Providing cybersecurity awareness to normal students may be relatively easy, but special needs students present unique challenges. Due to various types of disabilities, special needs students may struggle to understand the potential risks of using the internet or the importance of securing their devices and data. They may also have difficulty recognizing suspicious emails or messages and be more vulnerable to cybercriminals [8]. Cyberattacks such as phishing, ransomware, and malware can significantly disrupt the learning process and potentially impact a child's well-being. Despite perceiving the internet as safe, cyberattacks occur regularly, and victims often remain unaware. Special needs students, like all internet users, are vulnerable to cyber threats. However, their risk and vulnerability are greater than those of regular students [9].

Corresponding author. Email: hapini.awang@uum.edu.my

Humans are often the weakest link in the cybersecurity chain [10]. Their vulnerabilities frequently become attack points, revealing the need for cybersecurity awareness [11]. Therefore, it is crucial to educate them about potential threats and minimize their vulnerabilities, such as using weak passwords or insecure devices and applications. It is an essential component of education at all levels, and many European countries have already started implementing cybersecurity awareness programs, recognizing the need to advocate cybersecurity awareness among children, including those with special needs [12]. In Malaysia, cybersecurity education is not yet part of the formal curriculum. Surveys are needed to evaluate the current level of awareness and identify critical areas that should be included in educational programs. This study focused on special needs students in secondary schools to assess their level of cybersecurity awareness and recommend suitable parental control mechanisms. This study examined these demographic experiences, challenges, and requirements and was conducted among approximately 1.99 million students enrolled in government or government-aided secondary schools in Malaysia. Therefore, the objectives of this study are (i) to examine the level of internet usage, online activities, social media interactions, password management and phishing awareness, (ii) to investigate the level of parental control, and (iii) to analyse the correlation between internet usage, online activities, social media interactions, password management and phishing awareness.

2. LITERATURE REVIEW

In today's world, children and teenagers are increasingly vulnerable to cyberattacks due to their addiction to the internet [13], [14], [15]. This issue has been thoroughly discussed in the literature, as explained by the following examples of studies. [16] highlighted the importance of privacy literacy training for children and provided implications for policymakers and educators**,** while [17] explored the importance of understanding how families manage ***cybersecurity*** and negotiate boundaries in the digital age. Next, [18] guided educators and parents to teach children about responsible password use, as many mobile apps are designed for children. The researchers identified best practices for creating passwords and produced three age-appropriate password best practice guidelines as helpful ***resources***. Regarding younger children's understanding of online privacy risks and the need for adequate safeguards, [19] revealed that children could identify certain privacy risks, such as oversharing information and revealing real identities online, but were less aware of other risks***, such as*** tracking and game promotions. The study ***suggested*** the need for more support to enhance children's awareness of cyber risks and their ability to protect themselves online. Furthermore, [20] ***suggested*** using an interactive game to increase young people's awareness of privacy risks in social network activities. An experimental study involving 450 ***children*** and 22 teachers ***showed*** that the approach is practical. [21] also found similar findings when introducing The Adventures of ScriptKitty, a free online learning tool that teaches middle and high school students about essential network topics. The tool was piloted with 51 students, ***who showed*** significant improvement in their understanding of network topics and confidence in staying safe online. Next, [22] evaluated parental awareness of internet risks for their children. The results revealed an average level of parental awareness and emphasized the importance of parental education and involvement in promoting cyber safety at home. Another recent study of 420 schoolchildren ***proposed*** an integrated model of online safety based on constructs from protection motivation theory and the health belief model. The study ***revealed*** that engaging in safe online behavior requires children to have a high perception of the severity of online risks and knowledge of online privacy concerns [23]. One source of danger for children is their cyber-attack behaviour [15]. Suppose that a lack of awareness of cybersecurity risk exists. ***Therefore,*** personal information and privacy risk and cybersecurity threats, such as cyberbullying, online stranger danger, privacy, content, financial scams, and technical threats**,** may occur. ***Moreover, cybersecurity*** threats are becoming more widespread among children on the internet or in cyberspace [22], [24].

The importance of cybersecurity awareness has also been the topic of several previous studies [25], [26], [27], [28]. For example, first, [28] found that internet users in Israel, Slovenia, Poland, and Turkey have adequate cybersecurity awareness but apply minimal protective measures. This suggests that tailored training programs are necessary due to country-specific differences impacting the relationships among awareness, knowledge, and behavior. Second, [27] found that internet users in Slovenia, Poland, and Turkey have adequate cybersecurity awareness but apply minimal protective measures. This suggests that tailored training programs are necessary due to country-specific differences impacting the relationships among awareness, knowledge, and behavior. Third, [25] studied 423 adult smart home users in Japan and the UK and found that cultural factors significantly influence attitudes toward cybersecurity, impacting willingness to engage in training and preferences for nonfinancial incentives. While these and other studies, such as [13], [12], and [10], provide valuable insights into cybersecurity awareness and behavior among various populations, including university students and adult smart home users, there is a notable absence of research focusing specifically on special needs students. Ignoring this demographic overlooks groups facing unique challenges and vulnerabilities in navigating cybersecurity risks. Special needs students often require tailored educational approaches, and understanding their cybersecurity awareness and behaviors is crucial for developing effective interventions and support systems. It is vital to address this gap to ensure that all students, regardless of

their abilities, are safe in the digital world. This is an opportunity for policymakers to implement technical support and cybersecurity awareness programs tailored to these students' needs. Therefore, this study investigated the level of cybersecurity components, factors related to cybersecurity awareness, and parenting control among special needs students. The research is tailored to the experiences, challenges, and needs of special needs students in secondary schools regarding cybersecurity awareness and the role of parental controls in mitigating cyber threats for this particular demographic.

2.1 Research Model and Hypotheses

Based on a literature review and a focus group discussion with three cybersecurity experts, this study revealed that three independent variables can affect cybersecurity awareness among special needs students. These are internet Usage, Online Activities, and Social Media Interactions [4]. The study also identified two dependent variables, password management and situational phishing awareness, to measure the impact of these independent variables on an individual's online security [29], [30]. To measure the study's objectives, these variables are used as the background of the proposed research model (Fig. 1). The following hypotheses are tested following the study's stated goals and proposed model:

H1a *Internet usage has a significant correlation with password management.*

H1b *Internet usage has a significant correlation with situational phishing awareness.*

H2a *Online activities have a significant correlation with password management.*

H2b *Online activities have a significant correlation with situational phishing awareness.*

H3a *Social media interactions have a significant correlation with password management.*

H3b *Social media interactions have a significant correlation with situational phishing awareness*.

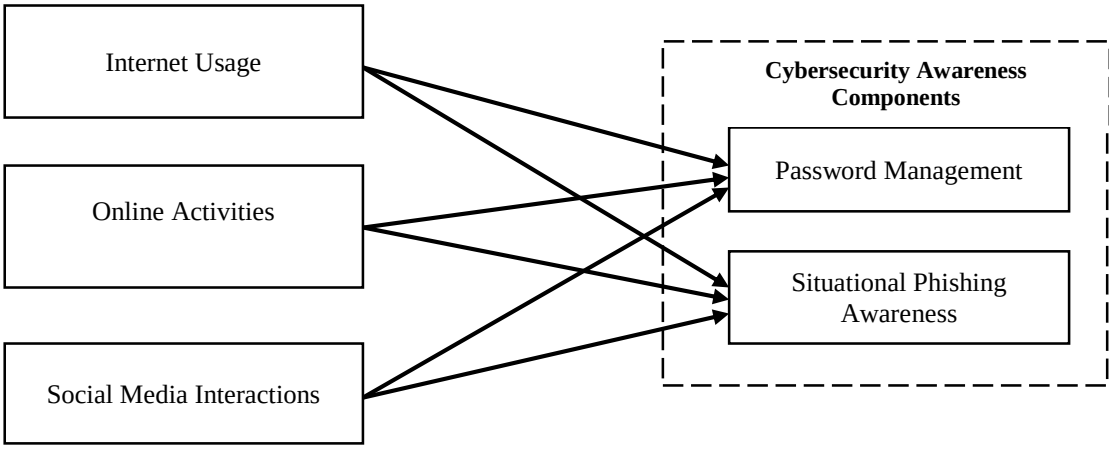

Fig. 1. The conceptual framework of the study

3. METHODOLOGY

The quantitative study utilized descriptive and inferential statistics based on primary data collected through a structured questionnaire. The survey in this study consisted of 29 questions covering various aspects related to internet usage, online activities, social media, phishing awareness, and password management. The questions were designed after conducting an extensive literature review and receiving input from cybersecurity experts to ensure their relevance and effectiveness. Before data collection, the questionnaire was pretested with 55 respondents to ensure its effectiveness. Convenience random sampling was used to collect the data, and demographic information was also collected. The responses were measured on a five-point Likert scale, where 5 indicated strong agreement and 1 indicated strong disagreement.

3.1 Participants

The study selected respondents who were students with disabilities in the *Program Pendidikan Khas Integrasi* (PPKI) in secondary schools across Malaysia. The selection process used stratified simple random sampling, which is a variation of simple random sampling. It involves dividing the population of secondary PPKI students into homogeneous groups called strata and selecting a simple random sample from each stratum. The schools were also sampled based on their urban or rural locations. As of 2021, the population size of secondary school PPKI enrolments was 33,901 [31]. Based on this

population size, this study employed Yamane's (1967) formula [32] to determine the minimum sample size needed. Given a population size (N) of 33,901 and a desired margin of error (e) of 5%, this study calculated the sample size (n) using the following formula:

$$n= N/(1+N(e^2))$$

This calculation yielded a sample size of approximately 396, which is required to achieve a representative and statistically significant sample. In this study, 438 people, representing 1.3% of the population, participated. This is a significant number, considering that many of the potential respondents have limitations that might prevent them from taking part in the survey. This study specifically selected PPKI students with mild disability who had access to the internet, ensuring equal representation of different genders and age groups within the secondary school category.

3.2 Data Analysis

The data gathered in this study were analysed using the Statistical Package for Social Sciences (SPSS). SPSS is an appropriate statistical tool for examining the collected data. Descriptive statistics were employed to describe the frequencies and percentages of the respondents' demographic profiles. The relationships between the variables were examined using correlation analysis. The hypotheses were tested using SPSS. The study's analysis is divided into two sections. The demographic information of the respondents was analysed in the first section. The second section examined the level of special needs students' awareness of specific components of cyberattacks, such as password management, online privacy, and phishing, which were investigated in the first section. During the data collection, 444 responses were gathered from special needs respondents in 1985 secondary schools across Malaysia with PPKI programs. Of these respondents, 51 answered in English and 393 answered in Malay. However, the data preparation and coding procedures generated 299 usable data points. One hundred thirty-nine patients were removed from the dataset due to incomplete or/and invalid responses. In addition to descriptive statistics, inferential statistics such as the Spearman rank correlation were also calculated in this study. Using G*Power software, the required sample size is determined and fulfilled, as only 159 cases are needed to conduct such analysis.

4. RESULTS AND DISCUSSION

4.1 Demographic Information of Respondents

The PPKI program in Malaysian secondary schools is designed for students aged between 13 and 19 years. The study classified the respondents' ages based on Malaysia's standard secondary school levels: lower and upper secondary. The lower secondary group consisted of PPKI students from Forms 1 to 3 aged between 13 and 15 years, while the upper secondary group included students aged between 16 and 19 years. Of the total respondents, 151 (50.5%) were lower secondary students, and 148 (49.5%) were upper secondary students. The 14-year-old age group was the most prominent, with 66 respondents accounting for 22.1% of all respondents, followed by the 16-year-old age group, with 65 respondents accounting for 21.7%. The least common age group was 19, with only 12 respondents, accounting for 4% of all respondents. Regarding gender, the study had a relatively balanced distribution, comprising 187 (62.5%) male and 112 (37.5%) PPKI students.

The study sampled 28 secondary schools with the PPKI program across Malaysia, with Kedah having the highest number of respondents at n=51 (17.1%), followed by Negeri Sembilan at n=36 (12%), Perak at n=31 (10.4%), and Labuan at n=30 (10%). On the other hand, Johor, Sabah, and Sarawak had the least number of respondents, at n=10 (3.3%), n=8 (2.7%), and n=1 (0.3%), respectively. The study also examined the locations of the schools, classifying them as either urban or rural areas. In summary, 237 (79.3%) PPKI students were from urban schools, while 62 (20%) were from rural schools. It is important to note that the study targeted students with mild disabilities who are capable of using technology, such as the internet, social media, and gadgets. Consequently, many respondents who fulfilled these criteria experienced learning problems (n=244, 81.6%). A total of 21 individuals (7%) had multiple disabilities, followed by 18 individuals (6%) with listening disabilities and 8 individuals (2.7%) with physical disabilities.

4.2 Internet Usage

According to a survey, 281 (94%) respondents accessed the internet from their homes. The increase in remote learning participation among students, including those in the PPKI program, was primarily influenced by the Movement Control Order (MCO) enforced in Malaysia during 2020 and 2021. However, a small number of respondents accessed the internet from other locations, such as schools (n=29, 9.7%), friends' and relatives' homes (n=25, 8.4%), public places such as restaurants, recreational parks, and shopping malls (n=25, 8.4%), and community internet centers (n=4, 1.3%).

The extent of internet usage among secondary PPKIs is defined based on three levels, namely, (i) mild: less than or equal to 4 hours, (ii) regular: between 5 and 12 hours, and (iii) heavy: more than 12 hours [33]. Thus, the majority of respondents fall into the mild category, comprising 130 individuals (44.1%), followed by moderate users, totaling 130 individuals

(43.5%). On the other hand, heavy internet users accounted for only 37 (12.4%) of all respondents. The crosstab analysis also revealed a greater percentage of heavy users among lower secondary, male and rural students in each category. Table I summarizes the cross-tabulation analysis of internet usage levels by school category, gender, and school location.

TABLE I. CROSS-TABULATION ON INTERNET USAGE LEVEL

Internet Usage Level	School Level				Gender				Location			
	Lower		Upper		Male		Female		Urban		Rural	
	n	%	n	%	n	%	n	%	n	%	n	%
Mild	68	22.7	64	21.4	82	27.4	50	16.7	103	34.4	29	9.7
Regular	60	20.1	70	23.4	84	28.1	46	15.4	111	37.1	130	43.5
Heavy	23	7.7	14	4.7	21	7.0	16	5.4	23	7.7	37	12.4
TOTAL	151	50.5	148	49.5	187	62.5	112	37.5	237	79.3	196	65.6

The majority of individuals surveyed fall into the "Mild" internet usage category, followed by the "Regular" category, and a smaller proportion fall into the "Heavy" category. Across both lower and upper school categories, there is a greater representation of "Regular" internet usage levels than "Mild" or "Heavy" levels. There is a somewhat balanced distribution between genders across different internet usage levels, with males having slightly higher levels of internet usage. Urban areas show more internet usage across all usage levels than do rural areas. Overall, internet usage among the surveyed population is predominantly moderate (regular), with variations observed based on school category, gender, and location.

4.3 Online Activities

This study creates a level of online activity based on three categories: mild, regular, and heavy. Table II describes the number of respondents based on the predetermined level. The activities included playing online games, downloading or watching online content, uploading content, chatting and interacting on social media, browsing social media sites, studying online, and shopping or selling online, categorized into three levels of engagement: mild, regular, and heavy. The results show that online gaming is a prevalent activity, with a considerable proportion of respondents engaging mildly (n=113, 37.8%), regularly (n=51, 17.1%), or heavily (n=135, 45.2%). Similarly, downloading or watching entertainment content is a widely practiced activity, with 109 (36.5%) respondents engaging mildly, 90 (30.1%) engaging regularly, and 100 (33.4%) engaging heavily. In contrast, uploading user-generated content portrays a slightly different pattern, with 144 (48.2%) participants engaging mildly, 86 (28.8%) engaging regularly, and 69 (23.1%) engaging heavily. Social interaction through chat messages and social media exhibits diverse engagement, with 127 (42.5%) individuals engaging mildly, 50 (16.7%) individuals engaging regularly, and 122 (40.8%) individuals being heavily involved. Browsing social media sites followed a similar trend, with 109 (36.5%) respondents mildly engaged, 55 (18.4%) regularly engaged, and 135 (45.2%) heavily involved. Moreover, online study showed a relatively balanced distribution across all engagement levels, with 91 (30.4%) individuals engaging mildly and 104 (34.8%) engaging regularly and heavily. Finally, online shopping or selling emerged as the most prevalent activity, with 226 (75.6%) participants mildly involved, 56 (18.7%) regularly involved, and 17 (5.7%) heavily involved. These findings provide valuable insights into the multifaceted digital behaviors of the surveyed population, indicating the need for nuanced approaches to fostering digital literacy and promoting safe online practices.

TABLE II. ONLINE ACTIVITIES LEVEL

Activity	Mild		Regular		Heavy		Total	
	n	%	n	%	n	%	n	%
Playing online games	113	37.8	51	17.1	135	45.2	299	100
Download/watch videos/movies/music/games for entertainment	109	36.5	90	30.1	100	33.4	299	100
Upload content videos/music/pictures/documents	144	48.2	86	28.8	69	23.1	299	100
Chat messages and interact on social media	127	42.5	50	16.7	122	40.8	299	100
Browse social media sites	109	36.5	55	18.4	135	45.2	299	100
Study online	91	30.4	104	34.8	104	34.8	299	100
Shop or Sell Online	226	75.6	56	18.7	17	5.7	299	100

4.4 Social Media Interactions

The study collected information about the people who created the social media accounts for the students. The respondents were allowed to choose more than one answer. A total of 145 (48.5%) were created by themselves. However, 122 (40.8%) had their social media created by their parents, and their siblings created 56 (18.7%). These were followed by friends (n=10, 3.3%) and people they knew (n=3, 1.0%). In terms of social media ownership, WhatsApp (n=247, 82.6%), YouTube (n=211, 70.6%) and Facebook (n=168, 56.2) are the top three platforms that secondary PPKI students own. On the other hand, high-risk social media platforms such as Bigo Live (n=6, 2.0%) and Sugarbook (n=1, 0.3%) are owned by only a minority of secondary PPKI students. Nevertheless, preventive actions still need to be taken, as these social media platforms are not intended to be their own PPKI students.

4.5 Password Management

The study also investigated students' awareness of creating secure passwords. They were asked to indicate whether their passwords contained numbers, lowercase, uppercase, special symbols or more than eight characters; 180 (60.2%) respondents included numbers in their passwords, and another 180 (60.2%) used uppercase characters. However, 227 (75.9%) respondents had never used special characters or symbols in their passwords, while another 167 (55.9%) had fewer than eight characters. Regarding special needs students' behaviors in managing their passwords, 73.2% never shared them with others, and 42.1% never wrote them in a notebook. Furthermore, 45.8% never repeated the same password in other social media accounts, while 33.1% never saved their phone passwords. However, 40.8% of the students often saved their passwords on their phones. A total of 28.1% of the students often and very often wrote their passwords in a notebook. Similarly, 23.1% used the same passwords for multiple social media accounts.

Table III shows the password management awareness levels among special needs students, categorized into four levels: very low, low, moderate, and high. A substantial proportion of respondents exhibited a moderate level of awareness, constituting 51.5% of the total sample. Meanwhile, 38.8% demonstrated high awareness, indicating a considerable understanding of password management practices. However, a notable portion of respondents (9.0%) exhibited low awareness, while only 0.7% demonstrated shallow awareness. These findings underscore the importance of enhancing password management education and promoting best practices to mitigate cybersecurity risks, particularly among those with lower awareness levels, to bolster overall digital security [34].

TABLE III. PASSWORD MANAGEMENT AWARENESS LEVEL

Password Management Awareness Level	Frequency	Percentage
Very Low	2	0.7
Low	27	9.0
Moderate	154	51.5
High	116	38.8
Total	299	100.0

4.6 Situational Phishing Awareness

This study also analysed the potential of special needs students for phishing attacks. The respondents were asked whether they had opened messages from unknown people, replied to messages from an unknown person, and were allowed apps to access their photos, location, contact and camera. Overall, 73.2% of the students never opened an email from an unknown person. In addition, 77.6% of the students never replied to emails from an unknown person, and 71.2% never allowed other apps to access their photos, location, contacts or camera. Furthermore, cross-tabulating phishing awareness levels among special needs students revealed insightful patterns across various demographic factors (Table IV). Among school categories, both lower and upper secondary categories show a gradual increase in awareness levels from very low to high, with the majority demonstrating moderate to high situational awareness.

Regarding gender, both males and females exhibited similar trends, with a slightly greater percentage of females showing high awareness. Urban areas generally display higher awareness levels than rural areas, with a notable proportion of students in urban locations demonstrating moderate to high awareness. Overall, a significant portion of special needs students demonstrated at least moderate phishing awareness, with values ranging from 9.7% to 62.9%, indicating the need for continued efforts to enhance cybersecurity education and awareness, particularly among students with lower levels of situational phishing awareness.

TABLE IV. CROSS-TABULATION OF SITUATIONAL PHISHING AWARENESS LEVEL

Situational Phishing Awareness	**School Category**								**Gender**								**Location**							
	Lower				Upper				Male				Female				Urban				Rural			
	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High
Frequency	0	1	29	121	0	5	20	123	0	4	25	158	0	2	24	86	0	5	44	188	0	1	5	56
Percentage	0.0	0.3	9.7	40.5	0.0	1.7	6.7	41.1	0.0	1.3	8.4	52.8	0.0	0.7	8.0	28.8	0.0	1.7	14.7	62.9	0.0	0.3	1.7	18.7

4.7 Parental Control

Next, the study investigated the parental control of the respondents through four questions. First, approximately 50.9% of the parents often and very often suggested ways of using the internet. Then, 47.9% of their parents helped them when something was difficult to do or find on the internet. Furthermore, 36.4% blocked or filtered some content on the internet. Finally, 42.2% limited the students' time on the internet. Cross-tabulating parental control levels among special needs students reveals significant insights into online safety practices across different demographic factors (Table V). Among school categories, 17 (5.7%) students in the lower category and 29 (9.7%) in the upper category had very low parental control levels, with a gradual increase of up to 59 (19.7%) and 62 (20.7%) students demonstrating high parental control levels, respectively. Similarly, across genders, 15 (5.0%) males and 34 (11.4%) females exhibited very low levels of parental control, while 96 (32.1%) females and 70 (23.4%) males demonstrated high levels of parental control. Regarding location, 21 (7.0%) students in rural areas and 50 (16.7%) in urban areas displayed very low levels, whereas 96 (32.1%) students in urban areas and 70 (23.4%) in rural areas demonstrated high levels. These findings underscore the importance of parental involvement in fostering a safer online environment for special needs students, emphasizing the need for continued efforts to promote effective parental control practices.

TABLE V. CROSS-TABULATION OF PARENTAL CONTROL LEVEL

Parental Control	**School Category**								**Gender**								**Location**							
	Lower				Upper				Male				Female				Urban				Rural			
	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High	Very Low	Low	Moderate	High
Frequency	17	29	46	59	15	34	51	48	22	38	65	62	10	25	32	45	21	50	70	96	11	13	27	11
Percentage	5.7	9.7	15.4	19.7	5.0	11.4	17.1	16.1	7.4	12.7	21.7	20.7	3.3	8.4	10.7	15.1	7.0	16.7	23.4	32.1	3.7	4.3	9.0	3.7

4.8 Hypothesis Testing

To test the proposed hypotheses, Spearman rank correlation analysis was applied. The results indicate that there is a negative correlation between internet usage and password management ($r(297)=-.130$, $p<0.05$), thus supporting H1a. Moreover, H1b is also supported by the findings, which demonstrate a negative correlation between internet usage and phishing awareness ($r(297)=-.125$, $p<0.05$). Next, it was observed that there was a negative correlation between downloading or streaming entertainment content and password management ($r(297)=-.121$, $p<0.05$). Similarly, a negative

correlation was found between uploading content and password management ($r(297)=-.197$, $p<0.05$). Based on these findings, it can be assumed that online activities have a negative impact on password management, thus supporting H2a. Additionally, there is a negative correlation between uploading content and phishing awareness ($r(297)=-.114$, $p<0.05$), which further supports hypothesis H2b. Finally, there is a negative correlation between Interaction in Social Media and Password Management ($r(297)=-.210$, $p<0.01$) and Phishing Awareness ($r(297)=-.299$, $p<0.01$), supporting both H3a and H3b. Table VI summarizes the findings of the hypotheses tested.

TABLE VI. HYPOTHESES TESTING

Hypothesis		**r**	**p**	Decision
H1a	Internet Usage	-.130	<0.05	Accepted
H1b	Internet Usage	-.125	<0.05	Accepted
H2a	Online Activities	-.121	<0.05	Accepted
H2b	Online Activities	-.197	<0.05	Accepted
H3a	Social Media Interactions	-.114	<0.01	Accepted
H3b	Social Media Interactions	-.210	<0.01	Accepted

Overall, the findings discussed in the previous sections suggest that cybersecurity awareness among people with special needs is still at an alarming level. Further interventions, especially from parents, are crucial and obviously needed. In addition, these findings shed light on another important hidden implication: the importance of campaigns to increase cybersecurity awareness in shaping the consumer electronic market. As young people are recognized as major contributors to digital product demand, they need to be educated in relation to their growth purchasing and consumption power [35]. Cybersecurity awareness campaigns among students, including those with special needs, will surely impact the consumer electronic market. As consumers become more aware of cybersecurity issues, product designers, developers, and manufacturers will be forced to provide better product security features, as elaborated in the next section. The study's findings can also significantly affect the consumer electronics market, particularly for special needs students. Fig. 2 abstractly shows that consumer electronics manufacturers can use this research to develop products that meet the cybersecurity needs of special needs students. Products could include parental control features and be designed to be easy to use for students with disabilities.

Figure 2 Visualization of the impact of cybersecurity awareness campaigns on the consumer electronic market

5. CONCLUSIONS AND IMPLICATIONS

The present study sheds light on cybersecurity awareness among special needs students and how it affects their satisfaction level with online activities. With the increasing use of the internet and online activities in the digital transformation era, it is essential to understand the implications of cybersecurity awareness among special needs students. The findings show that special needs students' level of awareness about cybersecurity has a significant impact on their satisfaction with online activities. This study identified password management and phishing as significant components of cybersecurity awareness.

Specifically, 60.2% of the students used numbers and uppercase characters in their passwords, 46.8% used lowercase characters, and 24.1% used special characters or symbols. Additionally, 44.1% of the students used passwords of fewer than eight characters, and 8.7% wrote their passwords in a notebook. Despite the moderate level of cybersecurity awareness among special needs students, the study revealed a significant knowledge gap that needs to be addressed. Therefore, tailored cybersecurity education ensures the safety and well-being of special needs students. The study also emphasized the importance of parental control in monitoring special needs students' online behavior to ensure their safety.

Additionally, the study highlights age as a factor in cybersecurity awareness, as older students tend to have a greater level of knowledge than younger students. Thus, schools should introduce cybersecurity education at an early age to provide students with a strong foundation for cyber-safety practices. In terms of the correlation between the drivers and components of cybersecurity awareness, the negative correlations found between online activities and password management, as well as between online activities and phishing awareness, have critical implications for individuals and organizations in terms of cybersecurity. These findings suggest that internet users who are special needs students should be educated and trained on how to manage their passwords securely, detect phishing attempts, and maintain safe online behavior. Education authorities such as the Ministry of Education and schools should also provide their students with effective cybersecurity training programs to minimize the risks of cyberattacks, data breaches, and other security incidents that may result from poor password management and lack of awareness. Moreover, this study highlights the need for further research to understand the underlying reasons behind these correlations and to develop more effective strategies to enhance cybersecurity in the digital age, especially among vulnerable groups such as special needs students.

Moreover, cyber threats and online risks pose greater risks to special needs students. The specific challenges they face in the digital world need to be identified to address these concerns. This can be done by conducting surveys and interviews with students, teachers, and parents to better understand their needs and experiences. Effective cybersecurity education programs tailored to the unique needs of special needs students must also be developed. Future research should focus on developing strategies to ensure that special needs students are protected from online risks and can navigate the digital world safely. The study concluded that special needs students' awareness of online services can be significantly increased by regular cybersecurity awareness camps, technical support, and necessary training and development.

Additionally, the research emphasizes the need for cybersecurity awareness programs tailored to the needs of special needs students in educational institutions. In summary, special needs students must be educated on the potential risks and dangers associated with using technology to ensure their safety. It is also crucial to actively involve parents and schools in monitoring special needs students' online activities to ensure their safety and well-being.

Funding
This research did not receive any financial support.

Conflicts of interest
The authors declare no conflicts of interest.

Acknowledgements
This study was conducted under the Institute for Advanced and Smart Digital Opportunities (IASDO), School of Computing, Universiti Utara Malaysia (UUM) Special Grant (SO Code: 21487). The authors would like to acknowledge all personnel who were involved and contributed to this study.

References

[1] S. Bannon, T. Mcglynn, K. Mckenzie, and E. Quayle, “Computers in Human Behavior The internet and young people with Additional Support Needs (ASN): Risk and safety,” *Comput. Human Behav.*, vol. 53, pp. 495–503, 2015, doi: 10.1016/j.chb.2014.12.057.

[2] M. M. Mijwil, Y. Filali, M. Aljanabi, M. Bounabi, and H. Al-Shahwani, “The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment,” *Mesopotamian J. CyberSecurity*, vol. 2023, pp. 1–6, 2023, doi: 10.58496/MJCS/2023/001.

[3] A. S. A. Albahri, Mohanad G. Yaseen, M. Aljanabi, A. H. A. Hussein Ali, and Akhmed Kaleel, “Securing Tomorrow: Navigating the Evolving Cybersecurity Landscape,” *Mesopotamian J. CyberSecurity*, vol. 2024, pp. 1–3, 2024, doi: 10.58496/mjcs/2024/001.

[4] C. G. Blackwood-Brown, "An Empirical Assessment of Senior Citizens' Cybersecurity Awareness,Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills.," *Nov. Southeast. Univ.*, no. 1047, pp. 1–275, 2018.

[5] G. Kassar, "Exploring cybersecurity awareness and resilience of SMEs amid the sudden shift to remote work during the Coronavirus Pandemic: A pilot study," *ARPHA Conf. Abstr.*, vol. 6, 2023, doi: 10.3897/aca.6.e107358.

[6] H. Awang, M. A. Zahurin, and S. O. Wan Rozaini, "Measuring Virtual Learning Environment Success from the Teacher's Perspective: Scale Development and Validation," in *Proceedings of the 3rd International Conference on Applied Science and Technology (ICAST'18)*, Penang, Malaysia: American Institute of Physics (AIP), 2018. doi: 10.1063/1.5055430.

[7] M. F. M. Yaakob, H. Awang, M. Z. Ismail, F. M. Zain, M. Kasim, and A. A. Z. Adnan, "Backward and Forward Reviews on Technical and Vocational Education and Training (TVET) in Malaysia: The Evolution and ICT-Driven Future Prospect," *Univers. J. Educ. Res.*, vol. 8, no. 6, pp. 2197–2203, 2020, doi: 10.13189/ujer.2020.080601.

[8] A. Deveci Topal, A. Kolburan Geçer, and E. Çoban Budak, "An analysis of the utility of digital materials for high school students with intellectual disability and their effects on academic success," *Univers. Access Inf. Soc.*, vol. 22, no. 1, pp. 95–110, 2023, doi: 10.1007/s10209-021-00840-0.

[9] A. El Asam and A. Katz, "Human – Computer Interaction Vulnerable Young People and Their Experience of Online Risks Vulnerable Young People and Their Experience of Online Risks," *Human–Computer Interact.*, vol. 00, no. 00, pp. 1–24, 2018, doi: 10.1080/07370024.2018.1437544.

[10] G. Ali and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare : State of the Art , Taxonomy , Mechanisms , and Essential Roles," *Mesopotamian J. CyberSecurity*, vol. 4, no. 2, pp. 20–62, 2024.

[11] M. Grobler and R. Gaire, "User , Usage and Usability : Rede fi ning Human Centric Cyber Security," vol. 4, no. March, pp. 1–18, 2021, doi: 10.3389/fdata.2021.583723.

[12] W. Liu, H. Xia, and J. Mou, "Understanding User's Continuous Use of Financial Technology Products," *Asia Pacific J. Inf. Syst.*, vol. 31, no. 2, pp. 236–256, 2021, doi: 10.14329/apjis.2021.31.2.236.

[13] F. Quayyum, D. S. Cruzes, and L. Jaccheri, "Cybersecurity awareness for children: A systematic literature review," *Int. J. Child-Computer Interact.*, vol. 30, p. 100343, 2021, doi: 10.1016/j.ijcci.2021.100343.

[14] Y. Yuliana, "the Importance of Cybersecurity Awareness for Children," *Lampung J. Int. Law*, vol. 4, no. 1, pp. 41–48, 2022, doi: 10.25041/lajil.v4i1.2526.

[15] A. Sadaghiani-tabrizi, "Revisiting Cybersecurity Awareness in the Midst of Disruptions Revisiting Cybersecurity Awareness in the Midst of Disruptions Supporting Global Business Education since 1901," *Int. J. Bus. Educ. Vol.*, vol. 163, no. 1, pp. 1–17, 2023, doi: 10.30707/IJBE163.1.1675491516.833197.

[16] L. Desimpelaere, L. Hudders, and D. Van de Sompel, "Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior," *Comput. Human Behav.*, vol. 110, no. 3, pp. 1–27, 2020, doi: 10.1016/j.chb.2020.106382.

[17] K. Muir and A. Joinson, "An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home," *Front. Psychol.*, vol. 11, no. 2, p. 425, 2020, doi: 10.3389/fpsyg.2020.00424.

[18] S. Renaud and P. Karen, "Age-appropriate password 'best practice' ontologies for early educators and parents," *Int. J. Child-Computer Interact.*, vol. 23–24, no. 5, pp. 1–27, 2020, doi: 10.1016/j.ijcci.2020.100169.

[19] J. Zhao *et al.*, "'I make up a silly name': Understanding children's perception of privacy risks online," in *Conference on Human Factors in Computing Systems - Proceedings*, 2019, pp. 1–13. doi: 10.1145/3290605.3300336.

[20] L. Bioglio, S. Capecchi, F. Peiretti, D. Sayed, A. Torasso, and R. G. Pensa, "A Social Network Simulation Game to Raise Awareness of Privacy among School Children," *IEEE Trans. Learn. Technol.*, vol. 12, no. 4, pp. 456–469, 2019, doi: 10.1109/TLT.2018.2881193.

[21] O. G. Baciu-Ureche, C. Sleeman, W. C. Moody, and S. J. Matthews, "The adventures of ScriptKitty: Using the Raspberry Pi to teach adolescents about internet safety," *SIGITE 2019 - Proc. 20th Annu. Conf. Inf. Technol. Educ.*, pp. 118–123, 2019, doi: 10.1145/3349266.3351399.

[22] N. A. Arifin, U. A. Mokhtar, Z. Hood, S. Tiun, and D. I. Jambari, "Parental awareness on cyber threats using social media," *J. Komun. Malaysian J. Commun.*, vol. 35, no. 2, pp. 485–498, 2019, doi: 10.17576/JKMJC-2019-3502-29.

[23] M. D. G. & M. S. H. Misha Teimouri, Seyed Rahim Benrazavi, "A Model of Online Protection to Reduce Children's Online Risk Exposure: Empirical Evidence From Asia," *Sex. Cult.*, vol. 22, no. 7, pp. 1205–1229, 2018, doi: 10.1007/s12119-018-9522-6.

[24] M. M. Mijwil, R. Doshi, K. K. Hiran, A. H. Al-Mistarehi, and M. Gök, "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," *Mesopotamian J. CyberSecurity*, vol. 2022, pp. 1–4, 2022, doi: 10.58496/MJCS/2022/001.

[25] N. Y. R. Douha, K. Renaud, Y. Taenaka, and Y. Kadobayashi, "Smart home cybersecurity awareness and behavioral incentives," *Inf. Comput. Secur.*, vol. 31, no. 5, pp. 545–575, 2023, doi: 10.1108/ICS-03-2023-0032.

[26] W. C. H. Hong, C. Y. Chi, J. Liu, Y. F. Zhang, V. N. L. Lei, and X. S. Xu, *The influence of social education level*

on cybersecurity awareness and behaviour: a comparative study of university students and working graduates, vol. 28, no. 1. Springer US, 2023. doi: 10.1007/s10639-022-11121-5.

[27] B. Ahamed *et al.*, "Empowering Students for Cybersecurity Awareness Management in the Emerging Digital Era: The Role of Cybersecurity Attitude in the 4.0 Industrial Revolution Era," *SAGE Open*, vol. 14, no. 1, pp. 1–14, 2024, doi: 10.1177/21582440241228920.

[28] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness , Knowledge and Behavior : A Comparative Study," *J. Comput. Inf. Syst.*, vol. 00, no. 00, pp. 1–16, 2022, doi: 10.1080/08874417.2020.1712269.

[29] L. Jaeger and A. Eckhardt, "Eyes wide open: The role of situational information security awareness for security-related behaviour," *Inf. Syst. J.*, vol. 31, no. 3, pp. 429–472, 2021, doi: 10.1111/isj.12317.

[30] D. Ondrušková and R. Pospíšil, "The good practices for implementation of cyber security education for school children," *Contemp. Educ. Technol.*, vol. 15, no. 3, 2023, doi: 10.30935/cedtech/13253.

[31] Kementerian Pendidikan Malaysia, "Buku Data Pendidikan Khas 2021," Putrajaya, Malaysia, 2021. [Online]. Available: https://www.moe.gov.my/en/muat-turun/pendidikankhas/buku-data-pendidikan-khas

[32] T. Yamane, *Statistics: An Introductory Analysis*, 2nd ed. New York: Harper and Row, 1967.

[33] Malaysian Communications and Multimedia Commission, "Internet Users Survey 2020," Cyberjaya, 2020. doi: ISSN 1823-2523.

[34] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Heliyon*, vol. 7, no. 1, 2021, doi: 10.1016/j.heliyon.2021.e06016.

[35] M. Shah, "Dynamics of Digital Marketing and Consumer Buying Behavior: A Quantitative Analysis," *J. Dev. Soc. Sci.*, vol. 4, no. II, 2023, doi: 10.47205/jdss.2023(4-ii)27.