Chinese School Boys and Social Media: A Study of Cyberattacks

Ying Wang

Recommended Citation:

Wang, Ying (2024). "Chinese School Boys and Social Media: A Study of Cyberattacks". *Profesional de la información*, v. 33, n. 2, e330216.

https://doi.org/10.3145/epi.2024.0216

Received on 2nd April 2024
Accepted on 6th July 2024

Ying Wang ✉
https://orcid.org/0009-0003-1557-447X
School for Marxism Studies
Shanxi University, Taiyuan
Shanxi, 030006, China
wy_911126@sina.com

Abstract

This study was conducted to measure the relationship between social media use and cyberattacks on students. The study also measures the moderating role of privacy issues, lack of information, and parental control concerning social media use and cyberattacks on students. The quantitative data was used in this research to measure the relationship between variables. Eight hundred fourteen responses were collected, and the respondents of this study were the students at a school located in Shanghai and its remote areas. The motivation of this research was to provide theoretical and practical findings to reduce the number of cyberattacks on students, which is necessary for their better social media use experience. The study analyzed the collected data using R language, a novel contribution to the literature. The direct and moderating relationships reported by this research were empirically analyzed to provide reliable findings in the literature. The study also recommends policy implications to keep students informed and away from cyberattacks.

Keywords

Cyberattacks, Cyberbullying, Social Media, Privacy Breach.

1. Introduction

The role of social media is essential in daily life. It provides the opportunity for the sharing of information and other purpose (**Baheer *et al.***, 2023). The information shared on social media platforms helps people understand their environment. However, the rapid information sharing on social media is also dangerous as fake information is shared on it (**Karthikeyan**, 2022). The sharing of counterfeit information and privacy breaches has become customary on social media. However, the problem of cyberbullying and cyberattacks is also standard on social media these days (**Thumronglaohapun *et al.***, 2022). The victims of these cyberattacks and cyberbullying are the students and teenagers. They face these challenges because they cannot protect their personal information on social media (**Razali; Nawang**, 2022). Similarly, the breach in social media information sharing is also a problem for its users as their confidential and personal information is in the wrong hands. The stability of information sharing on social media platforms can provide a way forward to avoid any possible cyberattacks (**Tiamboonprasert; Charoensukmongkol**, 2022; **Durmić *et al.***, 2020).

The students who use social media must have information about its privacy issues (**Wright; Wachs; Gámez-Guadix**, 2022). The available information on social media platforms can be problematic for students, reducing their behavior and learning. The information shared on social media platforms should not be personal and harmful (**Bedrosova *et al.***, 2022). The unfair use of information or privacy breaches on social media can cause cyberbullying to students. Many students who use social media face cyberbullying from their peers and strangers (**Schade; Voracek; Tran**, 2021). This cyberbullying is not good because people face challenges in it. However, the positive use of social media can benefit the students for community discussion and information sharing (**Chai**, 2021). The reliability of social media platforms used for cyberbullying can be a problematic factor. Many cases are reported each year regarding cyberattacks based on social media (**Chai**, 2021).

Previously, scholars reported different factors to avoid cyberattacks from using social media. **Houkamau *et al.*** (2021) pointed out that the students must be informed about the reliable use of social media to prevent cyberattacks. The

study **Kamel** (2021) pointed out that using social media platforms is critical for learning, but students must not share sensitive information. **Nappa *et al.*** (2021) remarked that personal information that could cause harm should not be shared on social media because the breach of privacy can be problematic to the students. The study **Carlson and Frazer** (2021) confirmed that using social media platforms is necessary in modern times. Still, users must be guided on how they can protect their data from those involved in cyberattacks. **Khudhair** (2021) highlighted that the social media platform administration must develop strict and robust protocols that cause hindrance in cyberattacks.

However, the current research aimed to measure the relationship between social media use and cyberattacks on students. The study also measures the moderating role of privacy issues, lack of information, and parental control about social media use and cyberattacks on students. The quantitative data was used in this research to measure the relationship between variables. The motivation of this research was to provide theoretical and practical findings to reduce the number of cyberattacks on students, which is necessary for their better social media use experience. The study analyzed the collected data using R language, a novel contribution to the literature. The direct and moderating relationships reported by this research were empirically analyzed to provide reliable findings in the literature. The rest of the study is divided into a review of the literature, the research methodology, the data analysis, and the discussion of hypotheses, findings, and implications. Furthermore, the future directions for scholars are also provided in this research.

2. Review of Literature

The use of social media has become a trend in modern times (**Albikawi**, 2023). However, the fair use of social media is required in contemporary times to ensure no public information breach. With the advancement of intelligent technology in mobile phones, the use of social media has also increased even among students (**Polanin *et al.***, 2021). For students using social media platforms rapidly, it becomes necessary for them to protect their data. The information sharing on social media platforms can cause students to learn, which is even problematic for their behavior (**Mahmood**, 2020). In this way, sincere work is required on social media platforms, and students must be guided in using social media. Information sharing on social media is common, but this information can be fake, which can affect the beliefs of the students (**Menin *et al.***, 2021). The students must understand the dynamics of their work and develop a positive approach to using social media. Cyberattacks on social media are common, and privacy protocols are required to avoid these attacks (**Zhu *et al.***, 2020). The students' motivation can become a significant factor in learning and improving students' behavior. A positive approach to students' behavior and learning can motivate them to advance their social values (**López-Meneses *et al.***, 2020). The reliability of social media platforms is necessary to ensure that students are learning to use social media correctly. The fair use of social media is helpful for students for information sharing. Still, the extensive use of social media can be problematic for them and even reduce their performance in education (**Vivolo-Kantor *et al.***, 2021). Therefore, social media platforms should be used carefully with appropriate working approaches, which are required to avoid any cyberattack (**Hellfeldt; López-Romero; Andershed**, 2020). The above discussion leads to the following hypothesis.

H1: Social media use has a relationship with cyberattacks on students.

The use of social media is necessary for the public as modern-day information is easy to access. However, the social media platforms working and monitoring is also required (**Yuvaraj *et al.***, 2021a). The breach in privacy on social media results in negative ways of information sharing, which is problematic for unstable information (**Forssell**, 2020). It is noted that the protocols for protecting the information on social media platforms should be appropriate, which is a way to improve learning. The strategic advancements in information protection on social media can become a significant factor for the public (**Barlett *et al.***, 2021). The reliability of information protection on social media is also necessary for the public. However, the developers should protect the social media-related information, which is necessary to lead social media in a better way (**Tahat; Tahat; Habes**, 2020). Users' experience with social media would be increased over time with the information protection protocols. The stability of information and its protection for the public is necessary to develop a positive attitude towards using social media (**Zhong *et al.***, 2021). Students spend a lot of time on social media platforms, which should be improved to enhance the public experience. Protecting information without any breach of privacy is a strategic way forward that can advance people's learning on social media applications (**Carlson; Frazer**, 2021). The stability of students in their learning and reliable performance is improved over time with sustainable working. The advancements in social media platforms should be based on the principles to avoid any breach of the privacy of the people (**Park *et al.***, 2021). It would be a way for the students to protect their information on social media platforms, which would help them achieve their goals strategically. The improvements in social media platforms can provide a way forward for the students in their better and more advanced user experience (**Ngo *et al.***, 2021; **Shadmanfaat *et al.***, 2021). The above discussion leads to the following hypothesis.

H2: Privacy issues moderate the relationship between social media use and cyberattacks on students.

The lack of information to use social media platforms is also a cause for students who face problems using social media (**Kircaburun *et al.***, 2021). Reliable working on social media platforms is necessary. Still, users must be aware of the use of social media. The information shared on social media platforms can be problematic for the users, but they must know how to use this information (**Khudhair**, 2021). The stability of the use of social media is also necessary to ensure that the

information is shared with users to improve their experience. The users of social media platforms must be provided with the guidelines required to develop their behavior positively (**Kamel**, 2021). Stability in using social media is necessary, which is possible by improving the users' behavior by providing them with reliable information. The information to use social media platforms helps the users to enhance their learning experience (**Nappa *et al.***, 2021). Furthermore, the use of social media platforms helps the users to get a better experience, which is also necessary for them to have stability in their work. The advancement of social media platforms is helpful for users to improve their understanding to get away from any cyberattacks (**Yuvaraj *et al.***, 2021b). Similarly, if teenagers are informed about the cheerful and careful use of social media, it would be helpful for them to enhance their performance. Stability in social media use can be a way forward to avoid any breach of privacy (**Zhong *et al.***, 2021). Therefore, user guidance for the social media platforms should be provided to each user, which would be helpful for advancement in the use of social media (**Tiamboonprasert; Charoensukmongkol**, 2022). The community groups for social media usage-related information sharing are also critical to advancing the use of social media for the public. The above discussion leads to the following hypothesis.

H3: Lack of information moderates the relationship between social media use and cyberattacks on students.

For children and students, it is the responsibility of the parents to provide information for the reliable use of social media (**Razali; Nawang**, 2022). Parents are required to teach their children how to use social media for information purposes only. The accounts of teenagers should be monitored by their parents to check for any potential threat to them regarding the use of social media (**Chai**, 2021). It would be a practical approach to advance the use of social media. When the students are using social media without the parents' permission, the parents' control is negligible, which causes the cyberbullying to the students (**Schade *et al.***, 2021). The advancements in social media platforms are necessary to develop social media's role strategically. Stability on social media platforms is possible with reliable work keenly required for parents (**Houkamau *et al.***, 2021). The proper monitoring of social media and discussion related to the use of social media with children can save them from cyberattacks. The mechanism for parental control on the use of social media should be appropriately developed, which would be helpful for the students to improve their usage (**Bedrosova *et al.***, 2022). Similarly, the students and children are also required to permit their parents to monitor their social media activities as it is a way forward for strategic development in it (**Karthikeyan**, 2022). The proper use of social media platforms is critical to learn, but it is also necessary to get away from cyberbullying and other attacks. Children who do not inform their parents about the breach of their information on social media platforms face challenges related to the violation of information, which is problematic for students to improve their behavior (**Thumronglaohapun *et al.***, 2022). Hence, the use of social media should be monitored appropriately, which is necessary to get away from cyberattacks (**Baheer *et al.***, 2023; **Todorov; Mitrev; Penev**, 2020). The above discussion leads to the following hypothesis.

H4: Lack of parental control moderates the relationship between social media use and cyberattacks on students.

3. Methodology

This research used A quantitative approach to measure the relationship between variables. This approach was used because the previous studies measured the same variables using quantitative data. Hence, the scale items developed, tested, used, and established from the earlier studies were used in this research to collect data (**Arpaci; Aslan**, 2023; **Mohamed; Ahmad**, 2012; **Ho *et al.***, 2020; **Zhang *et al.***, 2017; **Price *et al.***, 2018). The previous studies already established the validity of these scale items, and no pilot study was required for this purpose. However, external experts confirmed the face validity of the adapted scale to check the language and content of the scale. The experts confirmed the language of the scale was reasonable and understandable to the respondents. Hence, the scale of the study was validated. The questionnaires designed for this research were based on two sections. The first section was dedicated to the demographic information of the respondents. The second section of the questionnaire was designed for the Likert scale items. A five-point Likert scale was used for this purpose. This study considered a five-point Likert scale, regarded as non-confusing to respond to. The items adapted from the previous studies were used in this section to collect quantitative data to measure the relationship between variables.

The population of this study were students at different schools in China. The location of Shanghai and its remote areas were selected to collect the data. The schools were physically visited, and students were asked permission to collect data. The students ensured that they were ready to provide data for this research. Accordingly, permission was also obtained from the administration of schools to collect the data. The data was collected from students using a random sampling approach. This sampling method was applied because all the students were asked about their social media use. Accordingly, they also confirmed that they use social media. One thousand questionnaires were distributed at different schools to collect data. However, only 817 responses were collected back. The preliminary analysis was also conducted, and the study found 3 responses with missing values and biased responses. Hence, a sample of 814 respondents was finalized after removing the biased responses from the scale. Furthermore, the study used R language to analyze data, which is considered a new technique for quantitative and primary data analysis.

4. Data Analysis and Results

Initially, the normality of data was tested to measure its accuracy for further analysis. The study analyze the findings of

mean and standard deviation, which were reported as usual. Furthermore, the missing values were also tested and confirmed as expected. The study tested the skewness and kurtosis values to confirm the data's normality. The skewness and kurtosis values between +3 and -3 are reported as significant and usual (**Royston**, 1992). The results of the study shown in Table 1 pointed out that the skewness and kurtosis of the data were significantly established.

Table 1: Descriptive Statistics.

	Missing	Mean	Std. Deviation	Skewness	Std. Error of Skewness	Kurtosis	Std. Error of Kurtosis	Minimum	Maximum
SMU1	0	3.403	1.142	-0.125	0.169	-0.992	0.337	1.000	5.000
SMU2	0	3.330	1.176	-0.067	0.169	-1.050	0.337	1.000	5.000
SMU3	0	3.364	1.245	-0.153	0.169	-1.196	0.337	1.000	5.000
SMU4	0	3.427	1.194	-0.147	0.169	-1.104	0.337	1.000	5.000
SMU5	0	3.379	1.123	-0.100	0.169	-1.006	0.337	1.000	5.000
PI1	0	3.442	1.162	-0.131	0.169	-1.098	0.337	1.000	5.000
PI2	0	3.354	1.208	-0.006	0.169	-1.224	0.337	1.000	5.000
PI3	0	3.456	1.171	-0.198	0.169	-1.128	0.337	1.000	5.000
PI4	0	3.364	1.241	-0.010	0.169	-1.321	0.337	1.000	5.000
PI5	0	3.422	1.210	-0.125	0.169	-1.216	0.337	1.000	5.000
LI1	0	3.476	1.208	-0.127	0.169	-1.341	0.337	1.000	5.000
LI2	0	3.432	1.127	-0.128	0.169	-1.127	0.337	1.000	5.000
LI3	0	3.422	1.169	-0.134	0.169	-1.141	0.337	1.000	5.000
LI4	0	3.359	1.209	-0.151	0.169	-1.122	0.337	1.000	5.000
LI5	0	3.383	1.274	-0.151	0.169	-1.271	0.337	1.000	5.000
LPC1	0	3.350	1.191	-0.005	0.169	-1.232	0.337	1.000	5.000
LPC2	0	3.388	1.199	-0.153	0.169	-1.050	0.337	1.000	5.000
LPC3	0	3.320	1.106	0.059	0.169	-1.076	0.337	1.000	5.000
LPC4	0	3.393	1.240	-0.164	0.169	-1.197	0.337	1.000	5.000
CS1	0	3.451	1.208	-0.170	0.169	-1.192	0.337	1.000	5.000
CS2	0	3.519	1.180	-0.236	0.169	-1.232	0.337	1.000	5.000
CS3	0	3.325	1.196	-0.081	0.169	-1.023	0.337	1.000	5.000
CS4	0	3.316	1.246	-0.069	0.169	-1.220	0.337	1.000	5.000

CS = cyberattack on students, LPC = lack of parental control, LI = Lack of information, PI = privacy issues, and SMU = social media use

The findings of factor loadings were measured in the second stage. This analysis was conducted to measure the reliability of each scale item used in this research. The findings of factor loadings reported in Table 2 confirmed that all items achieved significant reliability, which was confirmed with p values. The p values less than 0.05 were accepted as substantial (**Hair *et al.***, 2010).

Table 2: Factor Loadings.

				95% Confidence Interval			
Latent	**Indicator**	**Estimate**	**Std. Error**	**z-value**	**p**	**Lower**	**Upper**
CS	CS1	1.000	0.000			1.000	1.000
	CS2	0.978	0.090	10.917	< .001	0.802	1.153
	CS3	0.988	0.091	10.892	< .001	0.810	1.166
	CS4	0.534	0.097	5.493	< .001	0.343	0.724
LI	LI1	1.000	0.000			1.000	1.000
	LI2	0.849	0.099	8.549	< .001	0.654	1.044
	LI3	0.912	0.103	8.842	< .001	0.710	1.114
	LI4	0.979	0.107	9.171	< .001	0.770	1.188
	LI5	1.116	0.113	9.874	< .001	0.894	1.337
LPC	LPC1	1.000	0.000			1.000	1.000
	LPC2	0.993	0.090	11.006	< .001	0.816	1.170
	LPC3	0.916	0.083	11.009	< .001	0.753	1.079
	LPC4	0.660	0.097	6.814	< .001	0.470	0.850
PI	PI1	1.000	0.000			1.000	1.000
	PI2	1.806	0.287	6.282	< .001	1.242	2.369
	PI3	1.852	0.289	6.400	< .001	1.285	2.419
	PI4	1.971	0.308	6.409	< .001	1.368	2.574
	PI5	1.948	0.303	6.435	< .001	1.355	2.542
SMU	SMU1	1.000	0.000			1.000	1.000
	SMU2	0.995	0.094	10.590	< .001	0.811	1.179
	SMU3	1.127	0.099	11.347	< .001	0.932	1.322
	SMU4	0.830	0.097	8.571	< .001	0.641	1.020
	SMU5	0.695	0.092	7.562	< .001	0.515	0.875

CS = cyberattack on students, LPC = lack of parental control, LI = Lack of information, PI = privacy issues, and SMU = social media use

Accordingly, the factor variance findings were determined. Factor analysis assumes that variance can be partitioned into two types of variances, common and unique. Common variance is the amount of variance that is shared among a set of items. Highly correlated items will share a lot of variances. The significant threshold to measure variance was $p < 0.05$. The findings shown in Table 3 confirmed that factor variance was significantly established.

Table 3: Factor Variances.

			95% Confidence Interval			
Variable	**Estimate**	**Std. Error**	**z-value**	**p**	**Lower**	**Upper**
SMU	0.777	0.125	6.229	< .001	0.533	1.022
PI	0.268	0.083	3.225	0.001	0.105	0.431
LI	0.714	0.129	5.541	< .001	0.461	0.966
LPC	0.849	0.135	6.278	< .001	0.584	1.113
CS	0.542	0.097	5.582	< .001	0.351	0.732

CS = cyberattack on students, LPC = lack of parental control, LI = Lack of information, PI = privacy issues, and SMU = social media use

Furthermore, the findings of residual variances were measured. Residual variance measures the amount of unexplained variance in the data. A high residual variance indicates a lot of variability in the data that is not accounted for by the model. The significant threshold to measure residual variance for each item was $p < 0.05$. The results of residual variance are shown in Table 4.

Table 4: Residual Variances.

			95% Confidence Interval			
Variable	**Estimate**	**Std. Error**	**z-value**	**p**	**Lower**	**Upper**
SMU1	0.521	0.067	7.790	< .001	0.390	0.653
SMU2	0.607	0.074	8.150	< .001	0.461	0.753
SMU3	0.555	0.076	7.333	< .001	0.407	0.703
SMU4	0.883	0.096	9.205	< .001	0.695	1.071
SMU5	0.879	0.093	9.488	< .001	0.698	1.061
PI1	1.076	0.109	9.885	< .001	0.863	1.289
PI2	0.579	0.068	8.522	< .001	0.446	0.712
PI3	0.446	0.056	7.913	< .001	0.336	0.556
PI4	0.492	0.063	7.851	< .001	0.369	0.615
PI5	0.441	0.058	7.641	< .001	0.328	0.554
LI1	0.740	0.082	9.033	< .001	0.579	0.900
LI2	0.751	0.080	9.371	< .001	0.594	0.907
LI3	0.767	0.083	9.266	< .001	0.605	0.929
LI4	0.769	0.084	9.126	< .001	0.604	0.934
LI5	0.727	0.083	8.708	< .001	0.563	0.890
LPC1	0.563	0.071	7.907	< .001	0.424	0.703
LPC2	0.595	0.074	8.065	< .001	0.451	0.740
LPC3	0.506	0.063	8.062	< .001	0.383	0.629
LPC4	1.160	0.120	9.691	< .001	0.925	1.394
CS1	0.550	0.078	7.047	< .001	0.397	0.703
CS2	0.524	0.074	7.037	< .001	0.378	0.670
CS3	0.544	0.077	7.084	< .001	0.393	0.694
CS4	1.290	0.132	9.791	< .001	1.031	1.548

CS = cyberattack on students, LPC = lack of parental control, LI = Lack of information, PI = privacy issues, and SMU = social media use

Finally, the findings of regression coefficients were used to analyze the data. The study found that the direct relationship between social media use and cyberattacks was significant, and H1 was accepted. Secondly, H2 was also established as the study found that privacy issues moderate the relationship between social media use and cyberattacks on students. Thirdly, H3 was also established as the study found that lack of information moderates the relationship between social media use and cyberattacks on students. Finally, H4 was also established as the study found that lack of parental control moderates the relationship between social media use and cyberattacks on students. The results of regression coefficients were accepted with $p < 0.05$ (**Hair *et al.***, 2017; **Hult *et al.***, 2018) and shown in Table 5.

Table 5: Regression Coefficients.

				95% Confidence Interval			
Predictor	**Outcome**	**Estimate**	**Std. Error**	**z-value**	**P**	**Lower**	**Upper**
SMU	CS	0.194	0.029	6.689	<.001	0.160	0.448
PI*SMU	CS	0.389	0.039	9.974	<.001	0.276	0.454
LI*SMU	CS	0.190	0.035	5.428	<.001	0.140	0.761
LPC*SMU	CS	0.504	0.055	9.163	<.001	0.114	0.172

CS = cyberattack on students, LPC = lack of parental control, LI = Lack of information, PI = privacy issues, and SMU = social media use

5. Discussion And Conclusion

This study considered empirical data to measure the relationship between variables. Empirical data was used for the analysis using the R language. The study found that the direct relationship between social media use and cyberattacks was significant, and H1 was accepted. Meanwhile, the findings of previous studies were used to compare the relationship established by this research. According to **Chai** (2021), using social media has become popular. Social media usage must be done responsibly to guarantee that public information is secure in the modern day. Student use of social media has expanded along with the introduction of intelligent technology in mobile phones. According to **Khudhair** (2021), students using social media frequently need to safeguard their personal information. Students' learning may

suffer due to information sharing on social networking platforms, which may have adverse behavioral effects. According to **Zhang; Han, and Ba** (2020), students need to be directed in their social media usage, and actual work is required to improve on social media platforms. Social media is a frequent place for people to share knowledge. However, some of this material may be false, which could challenge students' ideas. According to **Carlson and Frazer** (2021), in addition to developing a constructive social media usage strategy, students must comprehend the dynamics of their workplace. Social media hacks are frequent, and protecting oneself from them requires following privacy precautions. According to **Price *et al.*** (2018), students' motivation can significantly influence their ability to learn and change their behavior. Positive reinforcement in behavior and education can inspire pupils to improve their social values. According to **Nappa *et al.*** (2021), social media platforms must be dependable to guarantee that students acquire social media usage skills. According to **Kircaburun *et al.*** (2021), while students can benefit from the fair use of social media for knowledge exchange, excessive use of these platforms might negatively impact students' academic achievement. Social media platforms should be used properly and with the proper operating methods to prevent any cyberattack.

Secondly, H2 was also established as the study found that privacy issues moderate the relationship between social media use and cyberattacks on students. Meanwhile, the findings of previous studies were used to compare the relationship established by this research. According to **Arpaci and Aslan** (2023), the public must use social media because it is so easy to acquire information in the present era. Furthermore, social media networks need to be monitored and kept in operation. According to **Tahat *et al.*** (2020), social media privacy violations lead to unfavorable information dissemination, which is hazardous for unverified information. It is observed that adequate procedures for safeguarding data on social media platforms should be followed to advance learning. According to **Baheer *et al.*** (2023), the public may find the strategic social media information protection developments meaningful. The public also needs to be assured that information on social media is reliably protected. According to **Mohamed and Ahmad** (2012), to steer social media in a more positive direction, developers must safeguard information related to social media. Users would eventually have a better social media experience thanks to information protection procedures. According to **Ehman and Gross** (2019), information must be reliable protected to foster an exemplary attitude on social media usage. To improve the public's experience, social media platforms where students spend a lot of time should be upgraded. According to **Wachs; Wright, and Vazsonyi** (2019), one smart move that can help users learn more on social media platforms is to secure information while maintaining their privacy. With sustainable effort, pupils' learning and consistent performance become more stable. According to **Karthikeyan** (2022), social media platform innovations should be founded on protecting individuals' privacy against invasion. It would be a step in the right direction for the students to safeguard the data they post on social media sites, which would help them strategically accomplish their objectives. According to **Wright *et al.*** (2022), students may benefit from a more advanced and better user experience thanks to advancements in social media platform functionality.

Thirdly, H3 was also established as the study found that lack of information moderates the relationship between social media use and cyberattacks on students. Meanwhile, the findings of previous studies were used to compare the relationship established by this research. According to **Carlson and Frazer** (2021), students struggle with social media use due to a lack of knowledge about how to use these platforms. Users must know how to use social media, but dependable functioning on these sites is also essential. According to **Tiamboonprasert and Charoensukmongkol** (2022), social media platform users may have difficulties using the information posted there, but they must be aware of how to use it. Maintaining consistency in social media use is also essential to ensuring consumers receive information that enhances their experience. According to **Atapattu *et al.*** (2020), furnishing social media platform users with the requisite guidelines to foster positive behavioral development is imperative. Stability in social media use is essential, and it can be achieved by enhancing user behavior by providing trustworthy information. According to **Kircaburun *et al.*** (2021), the knowledge of how to use social media platforms aids users in improving their educational process. Utilizing social media sites also aids users in gaining a better experience, which is also required for them to have consistency in their work. According to **Houkamau *et al.*** (2021), social media platform advancements have helped users become more aware of how to avoid cyberattacks. In the same way, teens may improve their performance if they know how to utilize social media responsibly and constructively. According to **Kamel** (2021), maintaining consistency in social media use can help prevent privacy breaches. As a result, each user should receive user guidelines for the social media platforms since this will promote progress in using social media. According to **Forssell** (2020), to encourage the public's use of social media, community groups for information sharing relating to social media usage are essential.

Finally, H4 was also established as the study found that lack of parental control moderates the relationship between social media use and cyberattacks on students. Meanwhile, the findings of previous studies were used to compare the relationship established by this research. According to **Thumronglaohapun *et al.*** (2022), parents must educate their children and students on safe social media usage practices. Parents must instruct their children on using social media solely for informational purposes. According to **Ho *et al.*** (2020), parents should monitor their teenagers' social media profiles to see if anything could pose a risk to their safety. It would be a valuable strategy to promote social media usage. Parents have limited control over their children when they use social media without their consent, which leads to cyberbullying. According to **Thumronglaohapun *et al.*** (2022), the strategic development of social media's function requires advancing social media platforms. Stability on social networking platforms can be achieved through dependable

jobs, which is especially important for parents. According to **Zhang *et al.*** (2017), children can be protected from all cyberattacks by having appropriate social media monitoring and usage conversations. If the parental control system were built appropriately, it would benefit pupils to improve their social media usage. According to **Khudhair** (2021), as it's a step towards strategic growth, kids and students must also permit their parents to monitor their social media activity. While making appropriate use of social media is essential for learning, avoiding cyberbullying and other forms of abuse is equally vital. According to **Thumronglaohapun *et al.*** (2022), children who fail to notify their parents about the compromise of their data on social media sites encounter difficulties stemming from this information breach, which makes it difficult for pupils to behave better (**Albikawi**, 2023). Therefore, it's essential to monitor social media use in order to prevent cyberattacks adequately.

5.1. Implications and Future Directions

The study developed significant theoretical as well as practical implications. The findings of this research improved the body of knowledge because, previously, the relationship between these variables was inclusive. The study empirically found that social media use predicts cyberattacks on students. This relationship was reported as positive and negative by the findings of previous studies. Furthermore, the study also found that privacy issues positively moderate, strengthen, and improve the relationship between social media use and cyberattacks on students. Hence, this relationship is new to the body of knowledge because previous studies have not investigated this relationship. Accordingly, the study also found that lack of information positively moderates strengthens and improves the relationship between social media use and cyberattacks on students. Therefore, this relationship is new to the body of knowledge because previous studies have not investigated this relationship. Finally, the study also found that lack of parental control positively moderates strengthens and improves the relationship between social media use and cyberattacks on students. Hence, this relationship is new to the body of knowledge because previous studies have not investigated this relationship. Collectively, the study enriched the body of knowledge by highlighting the significant relationships between the variables.

The findings of this research also provide practical recommendations for students and their parents to avoid cyberattacks on social media platforms. Firstly, the study recommends protecting social media platforms to protect students from cyberattacks. The prime responsibility of social media developers is to provide strict security, which would help students to use social media safely. Furthermore, the students must be informed about the proper use of social media platforms. The information to use social media accounts is necessary for the students to protect them from cyberattacks. When the students are motivated to use social media, it is the responsibility of the parents to analyze the shared information on social media accounts. The collective efforts of the students and their parents are critically required to avoid this. The students should be motivated to use social media information critically and be trained not to share their sensitive information on social media platforms. It would be reliable for the students to advance their learning, which would be strategically important in improving their learning behavior. The awareness campaigns created for students to use social media reasonably would be helpful for them to be safe from any possible cyberattacks.

The findings of this research contributed significant knowledge to the literature. This research's critical theoretical contributions are reliable for advancing scholars' understanding. However, the study recommended future directions for the scholars to contribute to the literature. Future studies are required to conduct multigroup analysis to measure the way female and male students face challenges related to cyberbullying and cyberattacks on social media platforms. It would be a novel contribution to the literature by highlighting the significant findings. Accordingly, future studies are required to measure the impact of cyberbullying on the mental health of school students. This research should be conducted because previous studies left loops in the body of knowledge. In this way, this significant contribution would enrich the body of knowledge. The working on future studies in these directions would be substantial for future research to advance the body of literature.

References

Albikawi, Zainab Fatehi (2023). "Anxiety, Depression, Self-Esteem, Internet Addiction and Predictors of Cyberbullying and Cybervictimization among Female Nursing University Students: A Cross Sectional Study". *International Journal of Environmental Research and Public Health,* v. 20, n. 5, pp. 4293. *https://doi.org/10.3390/ijerph20054293*

Arpaci, Ibrahim; Aslan, Omer (2023). "Development of a Scale to Measure Cybercrime-Awareness on Social Media". *Journal of Computer Information Systems,* v. 63, n. 3, pp. 695-705. *https://doi.org/10.1080/08874417.2022.2101160*

Atapattu, Thushari; Herath, Mahen; Zhang, Georgia; Falkner, Katrina (2020). "Automated Detection of Cyberbullying Against Women and Immigrants and Cross-domain Adaptability". *arXiv preprint arXiv:2012.02565*. *https://doi.org/10.48550/arXiv.2012.02565*

Baheer, Rimsha; Khan, Kanwal Iqbal; Rafiq, Zeeshan; Rashid, Tayyiba (2023). "Impact of dark triad personality traits on turnover intention and mental health of employees through cyberbullying". *Cogent Business & Management,* v. 10, n. 1, pp. 2191777. *https://doi.org/10.1080/23311975.2023.2191777*

Barlett, Christopher P.; Seyfert, Luke W.; Simmers, Matthew M.; Hsueh Hua Chen, Vivian; Cavalcanti, Jaqueline Gomes; Krahé, Barbara; Suzuki, Kanae; Warburton, Wayne A.; Wong, Randy Yee Man; Pimentel, Carlos Eduardo (2021). "Cross-cultural similarities and differences in the theoretical predictors of cyberbullying perpetration: Results from a seven-country study". *Aggressive Behavior,* v. 47, n. 1, pp. 111-119. *https://doi.org/10.1002/ab.21923*

Bedrosova, Marie; Machackova, Hana; Šerek, Jan; Smahel, David; Blaya, Catherine (2022). "The relation between the cyberhate and cyberbullying experiences of adolescents in the Czech Republic, Poland, and Slovakia". *Computers in Human Behavior,* v. 126, pp. 107013. *https://doi.org/10.1016/j.chb.2021.107013*

Carlson, Bronwyn; Frazer, Ryan (2021). "Attending to Difference in Indigenous People's Experiences of Cyberbullying: Toward a Research Agenda." In: *The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies In Digital Crime, Technology and Social Harms).* Bailey, J.; Flynn, A.; Henry, N. (Eds.), pp. 145-163. Emerald Publishing Limited. *https://doi.org/10.1108/978-1-83982-848-520211008*

Chai, Lei (2021). "Does Religion Buffer Against the Detrimental Effect of Cyberbullying Victimization on Adults' Health and Well-Being? Evidence from the 2014 Canadian General Social Survey". *Journal of Interpersonal Violence,* v. 37, n. 21-22, pp. NP19983-NP20011. *https://doi.org/10.1177/08862605211050092*

Durmić, Elmina; Stević, Željko; Chatterjee, Prasenjit; Vasiljević, Marko; Tomašević, Milovan (2020). "Sustainable supplier selection using combined FUCOM–Rough SAW model". *Reports in Mechanical Engineering,* v. 1, n. 1, pp. 34-43. *https://doi.org/10.31181/rme200101034c*

Ehman, Anandi C.; Gross, Alan M. (2019). "Sexual Cyberbullying: Review, Critique, & Future Directions". *Aggression and Violent Behavior,* v. 44, pp. 80-87. *https://doi.org/10.1016/j.avb.2018.11.001*

Forssell, Rebecka Cowen (2020). "Gender and Organisational Position: Predicting Victimisation of Cyberbullying Behaviour in Working Life". *The International Journal of Human Resource Management,* v. 31, n. 16, pp. 2045-2064. *https://doi.org/10.1080/09585192.2018.1424018*

Hair, Joseph F; Anderson, Rolph E; Babin, Barry J; Black, Wiiliam C (2010). *Multivariate data analysis: A global perspective (Vol. 7)*. Upper Saddle River, NJ: Pearson.

Hair, Joseph F; Hult, G Tomas M; Ringle, Christian M; Sarstedt, Marko; Thiele, Kai Oliver (2017). "Mirror, Mirror on the Wall: A Comparative Evaluation of Composite-Based Structural Equation Modeling Methods". *Journal of the Academy of Marketing Science,* v. 45, pp. 616-632. *https://doi.org/10.1007/s11747-017-0517-x*

Hellfeldt, Karin; López-Romero, Laura; Andershed, Henrik (2020). "Cyberbullying and Psychological Well-being in Young Adolescence: The Potential Protective Mediation Effects of Social Support From Family, Friends, and Teachers". *International Journal of Environmental Research and Public Health,* v. 17, n. 1, pp. 45. *https://doi.org/10.3390/ijerph17010045*

Ho, Shirley; Lwin, May O.; Chen, Liang; Chen, Minyi (2020). "Development and Validation of a Parental Social Media Mediation Scale Across Child and Parent Samples". *Internet Research,* v. 30, n. 2, pp. 677-694. *https://doi.org/10.1108/INTR-02-2018-0061*

Houkamau, Carla; Satherley, Nicole; Stronge, Samantha; Wolfgramm, Rachel; Dell, Kiri; Mika, Jason; Newth, Jamie; Sibley, Chris G. (2021). "Cyberbullying Toward Māori Is Rife in New Zealand: Incidences and Demographic Differences in Experiences of Cyberbullying Among Māori". *Cyberpsychology, Behavior, and Social Networking,* v. 24, n. 12, pp. 822-830. *https://doi.org/10.1089/cyber.2020.0877*

Hult, G. Tomas M.; Hair Jr, Joseph F.; Proksch, Dorian; Sarstedt, Marko; Pinkwart, Andreas; Ringle, Christian M. (2018). "Addressing Endogeneity in International Marketing Applications of Partial Least Squares Structural Equation Modeling". *Journal of International Marketing,* v. 26, n. 3, pp. 1-21. *https://doi.org/10.1509/jim.17.0151*

Kamel, Ayat Abdel Khaleq (2021). "Improvement of a New Analysis Technique of phenomenon of bulling and Cyberbullying among Students at different stages". *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* v. 12, n. 7, pp. 3106-3115. *https://turcomat.org/index.php/turkbilmat/article/view/3927*

Karthikeyan, C. (2022). "Conceptualizing Causative Factors of Workplace Cyberbullying on Working Women." In: *Research Anthology on Changing Dynamics of Diversity and Safety in the Workforce.* pp. 164-184. IGI Global. *https://doi.org/10.4018/978-1-6684-2405-6.ch011*

Khudhair, Nibras Salim (2021). "Cyberbullying–A Critical Analysis of Laws, Criminal Responsibility and Jurisdiction". *Journal of Contemporary Issues in Business and Government,* v. 27, n. 3, pp. 2644-2644. *https://cibgp.com/au/index.php/1323-6903/article/view/1875*

Kircaburun, Kagan; Jonason, Peter; Griffiths, Mark D.; Aslanargun, Engin; Emirtekin, Emrah; Tosuntaş, Şule B.; Billieux, Joel (2021). "Childhood Emotional Abuse and Cyberbullying Perpetration: The Role of Dark Personality Traits". *Journal of Interpersonal Violence,* v. 36, n. 21-22, pp. NP11877-NP11893. *https://doi.org/10.1177/0886260519889930*

López-Meneses, Eloy; Vázquez-Cano, Esteban; González-Zamar, Mariana-Daniela; Abad-Segura, Emilio (2020). "Socioeconomic Effects in Cyberbullying: Global Research Trends in the Educational Context". *International Journal of Environmental Research and Public Health,* v. 17, n. 12, pp. 4369. *https://doi.org/10.3390/ijerph17124369*

Mahmood, Ibrahim Shakir (2020). "Are Cyberbullying Interventions and Criminal Law Prevention Effective?(A Review of Cyberullying Legislation in Iraq)". *PalArch's Journal of Archaeology of Egypt/Egyptology,* v. 17, n. 7, pp. 16983-16998. *https://archives.palarch.nl/index.php/jae/article/view/8899*

Menin, Damiano; Guarini, Annalisa; Mameli, Consuelo; Skrzypiec, Grace; Brighi, Antonella (2021). "Was that (cyber) bullying? Investigating the operational definitions of bullying and cyberbullying from adolescents' perspective". *International Journal of Clinical and Health Psychology,* v. 21, n. 2, pp. 100221-100221. *https://doi.org/10.1016/j.ijchp.2021.100221*

Mohamed, Norshidah; Ahmad, Ili Hawa (2012). "Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence From Malaysia". *Computers in Human Behavior,* v. 28, n. 6, pp. 2366-2375. *https://doi.org/10.1016/j.chb.2012.07.008*

Nappa, Maria Rosaria; Palladino, Benedetta Emanuela; Nocentini, Annalaura; Menesini, Ersilia (2021). "Do the Face-to-face Actions of Adults Have an Online Impact? The Effects of Parent and Teacher Responses on Cyberbullying Among Students". *European Journal of Developmental Psychology,* v. 18, n. 6, pp. 798-813. *https://doi.org/10.1080/17405629.2020.1860746*

Ngo, Anh Toan; Tran, Anh Quynh; Tran, Bach Xuan; Nguyen, Long Hoang; Hoang, Men Thi; Nguyen, Trang Huyen Thi; Doan, Linh Phuong; Vu, Giang Thu; Nguyen, Tu Huu; Do, Hoa Thi (2021). "Cyberbullying among school adolescents in an urban setting of a developing country: experience, coping strategies, and mediating effects of different support on psychological well-being". *Frontiers in Psychology,* v. 12, pp. 661919. *https://doi.org/10.3389/fpsyg.2021.661919*

Park, Ms- A.; Golden, Karen Jennifer; Vizcaino-Vickers, Samuel; Jidong, Dung; Raj, Sanjana (2021). "Sociocultural values, attitudes and risk factors associated with adolescent cyberbullying in East Asia: A systematic review". *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* v. 15, n. 1, pp. 5. *https://doi.org/10.5817/CP2021-1-5*

Polanin, Joshua R.; Espelage, Dorothy L.; Grotpeter, Jennifer K.; Ingram, Katherine; Michaelson, Laura; Spinney, Elizabeth; Valido, Alberto; Sheikh, America El; Torgal, Cagil; Robinson, Luz (2021). "A Systematic Review and Meta-analysis of Interventions to Decrease Cyberbullying Perpetration and Victimization". *Prevention Science,* v. 23, pp. 439-454. *https://doi.org/10.1007/s11121-021-01259-y*

Price, Ann M.; Devis, Kate; LeMoine, Gayle; Crouch, Sarah; South, Nicole; Hossain, Rosa (2018). "First year nursing students use of social media within education: Results of a survey". *Nurse Education Today,* v. 61, pp. 70-76. *https://doi.org/10.1016/j.nedt.2017.10.013*

Razali, Nurulhuda Ahmad; Nawang, Nazli Ismail (2022). "An Overview of the Legal Framework Governing Cyberbullying Among Children in Malaysia". *IIUM Law Journal,* v. 30, n. S1, pp. 207-228. *https://doi.org/10.31436/iiumlj.v30iS1.704*

Royston, Patrick (1992). "Which Measures of Skewness and Kurtosis Are Best?". *Statistics in Medicine,* v. 11, n. 3, pp. 333-343. *https://doi.org/10.1002/sim.4780110306*

Schade, Estelle C.; Voracek, Martin; Tran, Ulrich S. (2021). "The nexus of the dark triad personality traits with cyberbullying, empathy, and emotional intelligence: a structural-equation modeling approach". *Frontiers in Psychology,* v. 12, pp. 659282. *https://doi.org/10.3389/fpsyg.2021.659282*

Shadmanfaat, Seyyedeh Masoomeh; Choi, Jaeyong; Kabiri, Saeed; Lee, Julak (2021). "Impact of Social Concern on Cyberbullying Perpetration in Iran: Direct, Indirect, Mediating, and Conditioning Effects in Agnew's Social Concern Theory". *Deviant Behavior,* v. 42, n. 11, pp. 1436-1457. *https://doi.org/10.1080/01639625.2020.1753152*

Tahat, Dina Naser; Tahat, Khalaf Mohammad; Habes, Mohammad (2020). "Jordanian Newspapers Coverage of Cyberbullying during COVID 19 Pandemic". *PalArch's Journal of Archaeology of Egypt/Egyptology,* v. 17, n. 7, pp. 15390-15403. *https://archives.palarch.nl/index.php/jae/article/view/5939*

Thumronglaohapun, Salinee; Maneeton, Benchalak; Maneeton, Narong; Limpiti, Sasikarn; Manojai, Natthaporn; Chaijaruwanich, Jeerayut; Kummaraka, Unyamanee; Kardkasem, Ruethaichanok; Muangmool, Tanarat; Kawilapat, Suttipong (2022). "Awareness, Perception and Perpetration of Cyberbullying by High School Students and Undergraduates in Thailand". *PloS One,* v. 17, n. 4, pp. e0267702. *https://doi.org/10.1371/journal.pone.0267702*

Tiamboonprasert, Worakamol; Charoensukmongkol, Peerayuth (2022). *Effects of Ethical Leadership and Organizational Politics on Workplace Cyberbullying and Job Consequences of Employees in a Thai Educational Institution: Moderating Role of Political Skill of Employees.* National Institute of Development Administration. *https://repository.nida.ac.th/handle/662723737/5609*

Todorov, Todor; Mitrev, Rosen; Penev, Ivailo (2020). "Force analysis and kinematic optimization of a fluid valve driven by shape memory alloys". *Reports in Mechanical Engineering,* v. 1, n. 1, pp. 61-76. *https://doi.org/10.31181/rme200101061t*

Vivolo-Kantor, Alana M.; Niolon, Phyllis Holditch; Estefan, Lianne Fuino; Le, Vi Donna; Tracy, Allison J.; Latzman, Natasha E.; Little, Todd D.; Lang, Kyle M.; DeGue, Sarah; Tharp, Andra Teten (2021). "Middle School Effects of the Dating Matters® Comprehensive Teen Dating Violence Prevention Model on Physical Violence, Bullying, and Cyberbullying: a Cluster-Randomized Controlled Trial". *Prevention Science,* v. 22, n. 2, pp. 151-161. *https://doi.org/10.1007/s11121-019-01071-9*

Wachs, Sebastian; Wright, Michelle F.; Vazsonyi, Alexander T. (2019). "Understanding the Overlap Between Cyberbullying and Cyberhate Perpetration: Moderating Effects of Toxic Online Disinhibition". *Criminal Behaviour and Mental Health,* v. 29, n. 3, pp. 179-188. *https://doi.org/10.1002/cbm.2116*

Wright, Michelle F.; Wachs, Sebastian; Gámez-Guadix, Manuel (2022). "The Role of Perceived Gay-Straight Alliance Social Support in the Longitudinal Association Between Homophobic Cyberbullying and LGBTQIA Adolescents' Depressive and Anxiety Symptoms". *Journal of Youth and Adolescence,* v. 51, pp. 1388-1396. *https://doi.org/10.1007/s10964-022-01585-6*

Yuvaraj, N.; Srihari, K.; Dhiman, Gaurav; Somasundaram, K.; Sharma, Ashutosh; Rajeskannan, S.; Soni, Mukesh; Gaba, Gurjot Singh; AlZain, Mohammed A.; Masud, Mehedi (2021a). "Nature-Inspired-Based Approach for Automated Cyberbullying Classification on Multimedia Social Networking". *Mathematical Problems in Engineering,* v. 2021, n. 1, pp. 6644652. *https://doi.org/10.1155/2021/6644652*

Yuvaraj, Natarajan; Chang, Victor; Gobinathan, Balasubramanian; Pinagapani, Arulprakash; Kannan, Srihari; Dhiman, Gaurav; Rajan, Arsath Raja (2021b). "Automatic Detection of Cyberbullying Using Multi-feature Based Artificial Intelligence With Deep Decision Tree Classification". *Computers & Electrical Engineering,* v. 92, pp. 107186. *https://doi.org/10.1016/j.compeleceng.2021.107186*

Zhang, Xi; Han, Ziqiang; Ba, Zhanlong (2020). "Cyberbullying Involvement and Psychological Distress Among Chinese Adolescents: The Moderating Effects of Family Cohesion and School Cohesion". *International Journal of Environmental Research and Public Health,* v. 17, n. 23, pp. 8938. *https://doi.org/10.3390/ijerph17238938*

Zhang, Xingting; Wen, Dong; Liang, Jun; Lei, Jianbo (2017). "How the Public Uses Social Media Wechat to Obtain Health Information in China: A Survey Study". *BMC Medical Informatics and Decision Making,* v. 17, n. 2, pp. 66. *https://doi.org/10.1186/s12911-017-0470-0*

Zhong, Jinping; Zheng, Yunxiang; Huang, Xingyun; Mo, Dengxian; Gong, Jiaxin; Li, Mingyi; Huang, Jingxiu (2021). "Study of the Influencing Factors of Cyberbullying Among Chinese College Students Incorporated With Digital Citizenship: From the Perspective of Individual Students". *Frontiers in Psychology,* v. 12, pp. 576. *https://doi.org/10.3389/fpsyg.2021.621418*

Zhu, Xiao-Wei; Chu, Xiao-Wei; Zhang, Yan-Hong; Li, Zhen-Hua (2020). "Exposure to Online Game Violence and Cyberbullying among Chinese Adolescents: Normative Beliefs about Aggression as a Mediator and Trait Aggressiveness as a Moderator". *Journal of Aggression, Maltreatment & Trauma,* v. 29, n. 2, pp. 148-166. *https://doi.org/10.1080/10926771.2018.1550830*