The Effect of Social Media Engagement on Cybersecurity Behavior among Students of Hei's

Marife S. Briones[1], Althea L. Polestico[2], John Mark D. Tagalog[3], John Mark B. Lazaro[4,]

[1,2,3]Student, Santo Tomas College of Agriculture Sciences and Technology

[4]Instructor, Santo Tomas College of Agriculture Sciences and Technology

DOI: https://doi.org/10.47772/IJRISS.2026.100400273

Received: 15 April 2026; Accepted: 20 April 2026; Published: 06 May 2026

ABSTRACT

Cybersecurity behavior refers to how a person acts to protect devices, accounts, and personal information when using the internet and technology. This study aims to determine the significant relationship between social media engagement and cybersecurity behavior among students of a Higher Education Institution (HEI). Data were gathered from 359 students of HIE's in Santo Tomas, Davao del Norte. This study employed stratified random sampling and used quantitative, non-experimental research with a descriptive correlational design. The measurements used in this study were adapted from instruments that had been rigorously checked for accuracy and reference. The statistical tools used in this study were the mean and Pearson r. Findings showed that students exhibited high levels of social media engagement and cybersecurity behaviors, suggesting that these behaviors were often observed. The significance level of social media engagement among students of HEIs suggests that it has become a vital component of everyday academic and social lives. The strong connection between social media engagement and cybersecurity behavior suggests that higher social media engagement correlates with enhanced awareness and implementation of cybersecurity protocols.

Keywords: Social Media Engagement and Cybersecurity Behavior, Correlational Research Design, Philippines

INTRODUCTION

Cybersecurity behavior refers to the individual practices that reduce or mitigate the risk and probability of cyber threats (Almansoori et al., 2023). However, Pencheva et al. (2020) found that students ' involvement in cybercrime and cyberbullying is common, as some students believe that hacking is amusing. As stated by Kennison (2020), individuals' use of insecure cybersecurity behaviors, including the use of weak passwords, is a leading contributor to cybersecurity breaches. According to Parsons et al. (2020), cybersecurity behavior is influenced by individual differences in risk-taking, self-control, and attitudes toward security.

According to Alsharida et al. (2023), encouraging cybersecurity behaviors is essential to protect individuals at home and in the workplace against attacks. Similarly, Schaltegger et al. (2025) found that many serious cybersecurity incidents could be traced back to human behavior, either on the attacker's or the victim's side. Ransomware attacks are a prime example of a highly effective approach relying on an attacker's deliberate exploitation of a single human error. Moreover, Sajikumar and Ajithkumar (2023) highlight that human behaviors in online cyber activities have become a crucial area of research. Despite being relatively new, behavioral cybersecurity has gained considerable attention in academia and practical applications.

In the study conducted by Khan et al. (2024), social media engagement is linked with poor cybersecurity habits, such as poor passwords and the lack of antivirus programs, particularly among the younger population and students. Similarly, Petropoulou and Varouchas (2024) emphasized that social media engagement is linked to harmful behavior, as people share too many personal details that hackers misuse in social engineering schemes. Likewise, Nussipova and Slanbekova (2024) found that young people in Kazakhstan dedicate significant time to using social media sites, which affects cybersecurity behavior and perception towards online security threats.

Although social media is widely used, little research has been conducted to understand the differences in the impacts of diverse degrees of social media use on the cybersecurity behavior of individuals. The majority of available studies are technical and do not address the behavioral impacts of social media use. Such a gap demonstrates the urgency of the necessity to learn how online interactions could influence the awareness and behavior of users regarding digital safety. The rationale for conducting this study is that it could provide engineers with information to successfully measure and enhance responsible, safe online activities. This study on The Effect of Social Media Engagement on Cybersecurity Behavior Among Students of HEIs relates to SDG 4: Quality Education. To advance this objective, it could facilitate responsible online behavior and digital literacy, which are key to inclusive and safe learning in the digital era.

Statement of the Problem

This study aims to determine the significant relationship between social media engagement and cybersecurity behavior among students of HEIs. Specifically, this sought to answer the following questions:

What is the level of social media engagement in terms of:

1.1 social media platforms;

1.2 social media content; and

1.3 screen time?

What is the level of cybersecurity behavior in terms of:

2.1 behavior of using password;

2.2 data and information access;

2.3 device and internet/network usage;

2.4 social media practices; and

2.5 use of smartphone devices?

Is there a significant relationship between social media engagement and cybersecurity behavior among students of HEIs?

Hypothesis

The null hypothesis used a 0.05 level of significance, stating that there is no significant relationship between the effect of social media engagement and cybersecurity behavior among students of HEIs.

THEORETICAL FRAMEWORK

This theory is anchored on Protection Motivation Theory by Rogers (1975), which states that social media users who often face online risks or security alerts are likely to be encouraged to practice safer cybersecurity habits. Their awareness of potential threats and confidence in managing them determine how carefully they behave while using social platforms. This is also supported by Mousavi et al. (2020), who found that people's drive to protect their privacy on social media depends on how aware they are of potential risks and how much they trust the security features meant to keep their information safe.

Moreover, this theory is also anchored on Planned Behavior Theory by Ajzen (1991), which states that the intention of a person predicts behavior, and this intention is influenced by attitude towards behavior, subjective norms, and perceived behavioral control. It may assist in understanding how the attitudes held by the students towards cybersecurity, their perception of peer/social norms on social media, and their perceived ability to control

safe practices are the factors that motivate them to adopt cybersecurity behaviors. This is also supported by Goliath et al. (2024), who found that individual social media platforms could improve cybersecurity education, providing the students with information on cyber threats and cyber protection. This heightened awareness positively impacts their attitudes towards securing practices.

Conceptual Framework

The conceptual structure of the study's variables is shown in Figure 1. The independent variable is social media engagement with three indicators *the Social Media Platforms, Social Media Content, and Screen time (Ruiz et al., 2022). As stated by Wijayanto et al. (2020),* the dependent variable is cybersecurity behavior with five indicators: *the behavior of using passwords, data and information access, device and internet/network usage, social media practices, and use of smartphone devices*

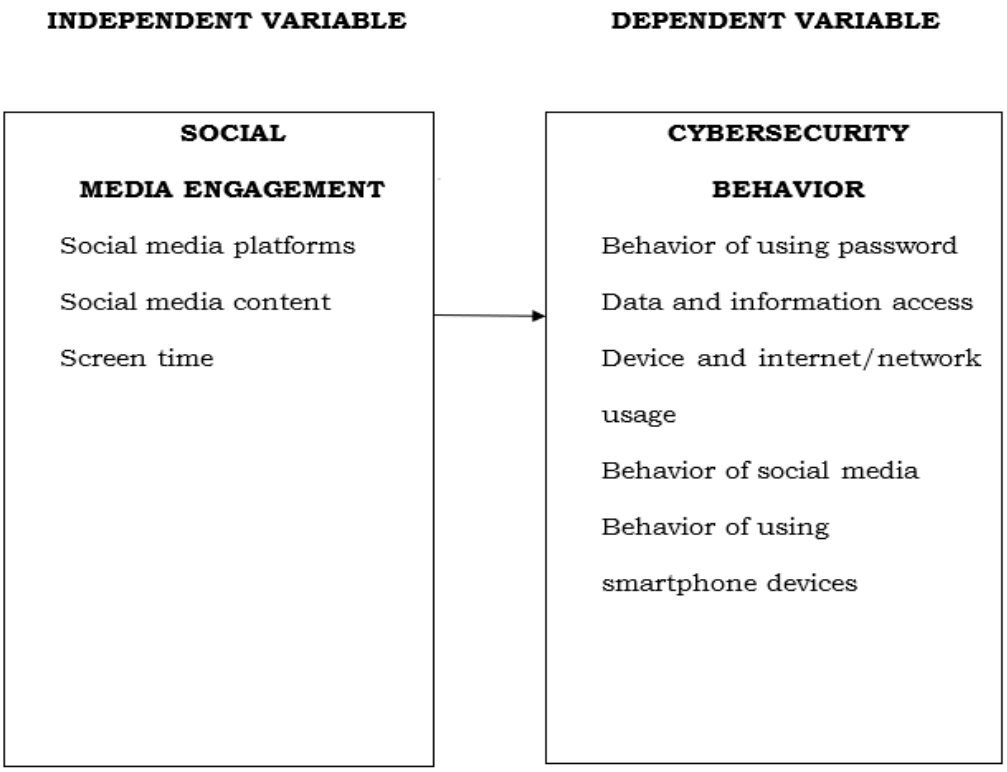

Figure 1. The Conceptual Paradigm of the Study

Significance of the Study

The result of the study is beneficial to the following entities and authorities:

Commission on Higher Education (CHED). The research is significant as it investigates the impact of social media use by students on the manner in which students manage online safety in Higher Education Institutions (HEIs). Since social media is a significant aspect of everyday and student life, this research sought to understand the impact of online activities on conscience and conduct regarding cybersecurity.

School Administrators. This study assists school administrators in realizing the impact of the use of social media by students on their cybersecurity behavior. Administrators in Higher Education Institutions (HEIs) may develop effective policies, training sessions, and awareness that urge students to conduct safe and responsible online actions. This is also likely to assist schools in enhancing data security and creating a more secure online learning space.

Teachers. This study would assist teachers in understanding the impact of students' social media practices on how they safeguard themselves online. Through an investigation into the connection between social media usage

and cybersecurity behavior, teachers would find more effective ways to show students how to use the internet wisely and safely. The results could also assist teachers in incorporating cybersecurity awareness in their courses so that students could learn how to think critically and acquire safe Internet skills.

Parents. This study is significant for parents because it provides insights into how their children's social media engagement relates to their children's cybersecurity behavior. When parents understand these connections, they could better guide their children in using social media responsibly and protecting their personal information online. The results of this research could help parents realize the importance of discussing online safety, privacy, and responsible digital practices at home. By doing so, parents become more involved in shaping their children's awareness, discipline, and decision-making in the digital world.

Students. The research is beneficial to students because it helps them understand how social media activities could contribute to Internet safety. With this understanding, students at Higher Education Institutions (HEIs) would be more conscious of what they post and how they interact across various platforms. This would also make them more responsible and conscious digital citizens with safer online habits.

Future Researcher. The result of the study benefits future researchers as a guideline and reference for their work. Its findings could help them investigate similar themes in social media use and cybersecurity behavior, and better understand how students' online activities impact security behavior.

Definition Of Terms

To ensure that all people comprehend the study, conceptual and operational definitions were provided for the following terminology:

Social Media Engagement. Social media engagement is defined as the individual attitude toward the relationship with social media use (Ni et al., 2020). In this study, it is operationally defined as the extent of engagement between students on social media, measured by liking, sharing, commenting, or posting content, and comprises three indicators: Social Media Platforms, Social Media Content, and Screen Time.

Social media platforms. This is the combination of internet applications that build on the technological foundations of Web 2.0, which allow the creation and exchange of user-generated content (Bokoh et al., 2022). In this study, web-based applications and tools are defined as those that enable people to create, share, and interact with digital materials and web communities.

Social media content. This is defined as the multitude of posts, videos, photos, and articles people share across social media platforms (Jadhav, 2024). In this study, social media content is defined as any text, picture, video, or interactive material posted by a user on social media to communicate, educate, or engage others.

Screen time. This is defined as the duration of time that is spent with any screen, such as phones, video games, televisions, computers, laptops, and tablets (Karani et al., 2022). In this study, this is defined as the total number of hours students spend on their phones, computers, televisions, and tablets per day, regardless of whether they are on social media, watching movies, or doing their studies.

Cybersecurity behavior. Refers to the actions, habits, and decisions made by individuals when using technology and information that affect the level of security of the data and systems they access (Latih & Zin, 2024). In this study, cybersecurity behavior is defined as the activities and habits that people show towards safeguarding data, equipment, and online accounts against potential online threats and security attacks.

Behavior of Using Password. Refers to how participants used and maintained passwords. The number of accounts and passwords owned, how often passwords are changed, and password recall strategies are part of password use behavior (Titiakarawongse & Boonkrong, 2023). In this study, it is defined how people manage and maintain passwords in their daily online behaviors. It is the number of passwords they have, the frequency with which they update passwords, and the manner in which they recall or store them.

Data and Information Access. It is the ability to identify, retrieve, and use information effectively (Tabuga, 2023). In this study, data and information access refers to the ease with which an individual could locate, extract, and utilize online digital information. It pays attention to the capabilities for accessing, handling, and applying trustworthy information, and to applying it to learning or decision-making, while considering privacy and security.

Device and Internet Usage. Refers to time spent using a mobile device such as a smartphone or tablet (Murdock & Heidenreich, 2021). Internet use is treated as a multidimensional concept comprising usage duration and types of online activities (Jiang, 2023). In this study, it is defined as the period during which students use electronic devices, such as smartphones and laptops, to conduct online tasks, including study, communication, and entertainment.

Social media practices. Refers to the set of routines and behaviors through which family firms engage with stakeholders via social media platforms (Obermayer et al., 2022). In this study, it is defined as the tactical practices and habits people employ to communicate and achieve objectives on social media sites. Practices involve posting, commenting, sharing, and managing the interactions, where the frequency and consistency across platforms measure them.

Use of smartphone devices. It is defined as the excessive use of mobile devices that negatively impacts academic, professional, and/or social functioning (Adamczewska, 2022). In this study, it is defined as the frequency and duration of time people spend using a handheld device, including calls, text messaging, internet access, social media, email, and gaming.

METHODOLOGY

This chapter presents the research design, research locale, research subject, research instrument, data collection, statistical tools, and ethical considerations to seek useful insights into the relationship between social media engagement and cybersecurity behavior among Higher Education Institutions.

Research Design

This study employed a quantitative, non-experimental, descriptive correlational research design to describe the quantitative data gathered on two variables related to social media engagement and cybersecurity behavior. As stated by Molina and Eduardo (2023), the systematic gathering of numerical information and statistical examination of it in order to comprehend and clarify phenomena, people, or occasions. It is found on the measurement and quantification of variables and analyzes the data with the help of statistical methods. According to Kotronoulas and Papadopoulou (2023), non-experimental quantitative research is an approach that focuses on describing situations or identifying relationships between variables without manipulating them. Moreover, Brodowicz (2024) explains that descriptive correlational research is mostly applied in situations where the researcher is interested in determining the features of specific groups of people or establishing a correlation between the variables. Descriptive correlational research, as noted by Bhat (2023), attempts to describe the relationship between two or more variables without making any statements about a cause-and-effect relationship.

This design enabled the researchers to collect numerical data through surveys and statistically analyze a substantial amount of data without manipulating variables. This study was devoted to describing and analyzing the current correlation between the frequency and intensity of social media platform use and their influence on students' online safety practices. Through this method, the research hypothesis sought to provide an impartial, evidence-based perspective on whether increased social media use affects students' awareness, attitudes, and behaviors regarding cybersecurity.

Research Locale

The study was done in Davao del Norte. The location is considered a first-class municipality. Santo Tomas is a landlocked municipality in the coastal province of Davao del Norte. The municipality has a land area of 221.80 square kilometers or 85.64 square miles, which constitutes 6.48% of Davao del Norte's total area. Its population,

as determined by the 2020 Census, was 128,667. This represented 11.44% of the total population of Davao del Norte province, or 2.45% of the overall population of the Davao Region. Based on these figures, the population density is 580 inhabitants per square kilometer, or 1,502 inhabitants per square mile. Geographically, Santo Tomas is on the island of Mindanao and in the province's second political district. It borders the north with the Municipalities of Kapalong and Talaingod, the east with the municipality of Asuncion, the west with Davao City, and the south with the Municipality of Braulio E. Dujali. This was called in honor of Saint Thomas, patron saint of Danao, the hometown of the late governor of undivided Davao Province, Vicente Duterte, father of the 16th Philippine President, Rodrigo R. Duterte.

It was originally known as Tibal-og and was once under the jurisdiction of the local town of Kapalong. The area was originally a tropical forest where the local Ata-Manobo people lived before the 1950s. It was home to a different culture, mixing Mandaya and Ata-Manobo.

This study was conducted in the Municipality of Santo Tomas, Davao del Norte, where college students from local higher education institutions served as respondents. This location was selected because Santo Tomas has several colleges with large student populations who are considered knowledgeable and capable of providing meaningful insights for the research.

Figure 2. Map of the Philippines Highlighting the Municipality of Santo Tomas

Research Subject

The respondents of this study comprise 359 of a total of 5,323 higher education institution (HEI) students enrolled in Santo Tomas, Davao del Norte. The researcher used Raosoft calculator, an online tool for determining sample size, to calculate the appropriate number of respondents based on the total population. To ensure that various groups within the population are fairly represented, respondents were selected using stratified random sampling. As stated by Nguyen et al. (2021), stratified random sampling offers the advantage of focusing on a few strata rather than the entire population by regulating the distribution of sample sizes. For example, a stratum with a large standard deviation will get more allocation compared to a stratum with a smaller one.

Research Instrument

The researchers used two (2) modified adapted survey questionnaires for the independent dependent variable. The questionnaires were validated by the panelist and an external validator to ensure their validity.

Social Media Engagement Questionnaire

The questionnaire was used to get the level of Social Media Engagement, which is from the research study titled "Social Media Engagement: Its Relation to the Psychosocial Attributes of Selected Junior High School Students" (Ruiz & Cabigan, 2022). The questionnaire consists of 11 items covering the following aspects: Social Media Platform (5 items), Social Media Content (5 items), and Screen time (1 item). Respondents rated each item using a 5-point Likert scale, from 5 for "always observed", 4 for "oftentimes observed", 3 for "sometimes observed", 2 for "seldom observed", and 1 for "least observed".

The parameters used for the interpretation of social media engagement and cybersecurity behavior among HEI students studying at a local higher education institution in Santo Tomas, Davao del Norte, were the following:

Range of Mean	Descriptive Level	Interpretation
4.20 – 5.00	Very High	Social media engagement was always observed
3.40 – 4.19	High	Social media engagement was oftentimes observed
2.60 – 3.39	Moderate	Social media engagement was sometimes observed
1.80 – 2.59	Low	Social media engagement was seldom observed
1.00 – 1.79	Very Low	Social media engagement was least observed

Cybersecurity Behavior Questionnaire

The questionnaire was used to assess the level of social media engagement in the research study titled "Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic" (Wijayanto & Prabowo, 2020).

The questionnaire consists of 33 items covering the following aspects: Behavior of Using Password (6 items), Data and Information Access (7 items), Device and Internet / Network Usage (7 items), Social Media (7 items), Using Smartphone Devices (6 items). Respondents rated each item using a 5-point Likert scale, from 5 for "always observed", 4 for "oftentimes observed", 3 for "sometimes observed", 2 for "seldom observed", and 1 for "least observed".

The parameter used for the interpretation of social media engagement and cybersecurity behavior among HEI's students studying at a local higher education institution in Santo Tomas, Davao del Norte were the following:

Range of Mean	Descriptive Level	Interpretation
4.20 – 5.00	Very High	Cybersecurity behavior was always observed
3.40 – 4.19	High	Cybersecurity behavior was oftentimes observed
2.60 – 3.39	Moderate	Cybersecurity behavior was sometimes observed
1.80 – 2.59	Low	Cybersecurity behavior was seldom observed
1.00 – 1.79	Very Low	Cybersecurity behavior was least observed

Data Collection

The following procedures were followed by the researchers in order to gather the data:

Obtaining permission to undertake the research. The researchers obtained the permission of the Research Director and Development before commencing the study to gather information. The research questionnaire has been carefully assessed and checked by the experts to ascertain its accuracy and credibility. Also, the researchers received an Ethics Certificate, thereby enabling the official investigation of the study and ensuring that all data collection was ethically sound.

Asking the respondents to give consent. All participants were given informed consent forms before the data collection process began. The research was conducted with strict adherence to data privacy and security, guided by the study's strong ethical principles to guarantee the well-being, justice, and dignity of all participants. The nature of transparency and free involvement of the participants in the study is achieved by explaining the purpose of the study, the roles of participants, and the intended use of the data.

Distribution and Retrieval of questionnaires. Upon receiving approval, the researchers gave the research instruments to the participants in person. To safeguard the validity and reliability of the research, they were keen to monitor the distribution and retrieval of the questionnaires so that participants would provide comprehensive and accurate answers.

Gathering and Interpretation of Data. Once the completed research instruments were collected, the researchers sorted, summarized, and tabulated the data. In the data analysis process, the researcher liaises with experienced statisticians to ensure that the interpretation of the results is accurate and reliable.

Ethical Consideration

Social Value. The study promotes social value by examining how social media engagement affects cybersecurity behavior among HEI students, addressing concerns about online safety. Its findings could help educators improve digital literacy programs and encourage responsible online practices for a safer society.

Informed Consent. In this study, informed consent was obtained from all participants through a clear and truthful consent form, either in print or via a secure online platform, which outlined the research purpose, procedures, risks, benefits, data use, and participants' rights. Participants were fully informed in simple language, with emphasis on voluntary participation, no coercion or inducement, and the right to withdraw at any time.

Vulnerability of Research Participants. The participants in this study were not highly vulnerable, as they were students able to provide informed and voluntary responses, but their protection was ensured by maintaining strict anonymity. Data were collected in a setting free from the influence of authority, such as when teachers were not present, to ensure students felt safe, unpressured, and able to respond honestly.

Risk, Benefits, and Safety. The study poses minimal risk to participants, with any potential discomfort from reflecting on online behavior reduced by using non-invasive survey items focused on general cybersecurity practices. These minimal risks were outweighed by the benefits, as the findings could enhance students' digital safety and guide institutions in promoting responsible social media use.

Data Privacy and Confidentiality. The study protects data privacy and confidentiality by collecting only necessary information and ensuring that participants' identities are never revealed in any reports or presentations. Responses are voluntary, participants may skip questions or withdraw at any time, and all records will be securely stored in password-protected digital files and locked cabinets for hard copies.

Justice. The study adheres to the principles of justice by selecting respondents fairly, treating all participants equally, and covering any participation-related expenses. It also ensures a fair balance of risks and benefits through rigorous academic review and validation of research tools.

Transparency. The study upholds transparency by fully informing participants about the purpose and nature of their involvement, allowing them to make an informed decision. Participants could access the results upon request, and all findings accurately reflect the collected data without alteration.

Adequacy of Facilities. The study adhered to the ethical principle of adequate facilities by ensuring the researcher had access to necessary resources, including library materials, a reliable laptop, and stable internet access. These resources allow the study to be conducted efficiently and responsibly, maintaining data quality and participant welfare.

Community Involvement. The study promotes community involvement by engaging the academic community—panel members, administrators, teachers, and students—in validating the research and interpreting findings, while sharing results in conferences and LAC sessions. These insights help school authorities design targeted cybersecurity programs that foster safer digital practices and benefit society.

RESULTS

The data presented, evaluated, and interpreted in this section are based on the research objectives. The following is the sequence in which the following topics are discussed: level of social media engagement, level of cybersecurity behavior among students of HEIs, and the significant relationship between social media engagement and cybersecurity behavior among students of HEIs.

Level of Social Media Engagement among Students of HEIs

The descriptive statistics for determining the level of social media engagement are shown in Table 1, with an overall mean of 4.10 and a standard deviation (SD) of 0.84, indicating a high level of engagement. This means that the students' social media engagement at HEIs is often observed. It also shows in the result that *Social Media platforms have the highest* mean of 4.18 and SD of 0.79 with a descriptive level of high, which means social media platforms are oftentimes observed. This means that the highest mean indicates that social media platforms are often seen as tools students actively use for learning, positive interaction, personal well-being, and maintaining privacy and security online. On the other hand, *Screen time* has the lowest mean of 4.01 and an SD of 0.91, with a descriptive level of high, indicating that screen time is often observed. This means that the lowest indicator shows that although students often set time limits on playing games, this behavior is the least consistently practiced among the indicators, implying that screen time remains frequently observed despite a generally high level of self-regulation.

Table 1 Level of social media engagement

Indicators	Mean	SD	Descriptive Equivalent
1. Social media platforms	4.18	0.79	High
2. Social media content	4.12	0.83	High
3. Screen time	4.01	0.91	High
Overall	**4.10**	**0.84**	**High**

Level of Cybersecurity Behavior among Students of HEIs

The statistical results on determining the level of cybersecurity behavior are shown in Table 2, which has an overall mean of 3.80 and an SD of 1.08, described as high. This means that the students' cybersecurity behavior in HEI is oftentimes observed. It also shows in the result that the Behavior of Using Passwords has the highest mean of 4.09 and SD of 0.99 with a descriptive level of high, which means behavior of using passwords is oftentimes observed. This means that the highest mean indicates that students often practice password-related

security behaviors, suggesting a generally strong awareness of and adherence to account protection measures in their digital activities. In contrast, Behavior of Social Media has the lowest mean of 3.63 and SD of 1.27, with a descriptive level of high, which means behavior of social media is oftentimes observed. This means that the lowest indicator indicates that although social media practices are often observed, some behaviors are less consistently performed, indicating variability in how frequently students engage in certain social media activities.

Table 2 Level of cybersecurity behavior

Indicators	Mean	SD	Descriptive Equivalent
1. Behavior of using password	4.09	0.99	High
2. Data and information access	3.77	1.05	High
3. Device and internet/network usage	3.68	1.11	High
4. Behavior of social media	3.63	1.27	High
5. Behavior of using smartphone devices	3.84	0.99	High
Overall	**3.80**	**1.08**	**High**

Significant relationship between Social Media Engagement and Cybersecurity Behavior among Students of HEIs

Displayed in Table 3 is the relationship between the independent variable (Social Media Engagement) and the dependent variable (Cybersecurity Behavior). The overall coefficient of correlation is .515, with a p<value of 0.001, which is lower than the 0.05 level of significance. This means a significant relationship exists between social media engagement and cybersecurity behavior since the probability value is p<0.001. Thus, the null hypothesis of no significant relationship is therefore rejected. The overall correlation coefficient of .515 also showed that there is a medium positive correlation between the two variables, which are the social media engagement and cybersecurity behavior.

Table 3. Significance of the relationship between social media engagement and cybersecurity behavior

Variables Correlated	Mean	r	p-value	Decision on H_o	Decision on Relationship
Social media engagement	4.10				
Cybersecurity behavior	3.80				
		0.515**	<0.001	Rejected	Significant

DISCUSSION

This chapter discussed the review, conclusion, and recommendations based on the research results were presented and the significance of the relationship between social media engagement and cybersecurity behavior among students of HEI's was discussed.

Level of Social Media Engagement among Students of HEI's

The result revealed that students of HEI's have a high level of Social Media Engagement, which means social media engagement is often observed. This means that the result implies students of HEIs are highly active on social media, indicating that social media engagement is frequently observed in their daily academic and personal activities.

The findings confirm the claim of Manur et al. (2023) that social media engagement enhance collaborative learning and academic engagement through interactive features such as discussion forums and peer-to-peer communication that help students share and reinforce academic information. It is also supported by Bindra and DeCuir-Gunby (2020), who found that social media use among college students extends to engagement with race-related issues, with moral identity influencing how students interact with such content online. Moreover, Parrott and Okojie (2024) emphasized that social media strengthens social connectedness and campus involvement particularly in Historically Black Colleges and Universities (HBCUs) by supporting student communication and collaboration.

Level of Cybersecurity Behavior among Students of HEI's

The findings showed that students of HEI's have a high level of Cybersecurity Behavior, which means cybersecurity behavior is often observed. The result implies that students of HEI's frequently practice cybersecurity behaviors, indicating a generally high level of awareness and responsible digital practices in their online activities.

The findings confirm the statement of Goliath et al. (2024) that specific skill deficiencies, especially among undergraduate students, can be addressed through customized educational programs to improve their cybersecurity resilience. It is also supported by Marques and Sousa (2023) that simulated phishing attacks and awareness campaigns have been used to advance students' knowledge of cyber threats. Additionally, Deuri (2025) supported that the use of complex passwords and two-factor authentication can become a significant way to mitigate weaknesses.

Relationship between Social Media Engagement and Cybersecurity Behavior among Students of HEI's

The relationships between two variables were tested in this study. This is between independent and dependent variables. The independent variable in this study is social media engagement and the dependent variable in this study is cybersecurity behavior. The relationship test found a statistically significant association between the evaluated variables.

The relationship analysis between social media engagement and cybersecurity behavior revealed a medium positive correlation. Moreover, social media engagement and cybersecurity behavior revealed a significant relationship since the probability value is $p<0.001$, lower than the 0.05 level of significant. The findings affirm the statement of Nussipova & Slanbekova (2024), which stated that the social media engagement among young people is great and that the media can influence the behavior and views of young people towards the dangers of cybersecurity.

Also, the result affirms the statement of Choi & Thompson (2025), that the more people are aware of media reporting on privacy risks, the better the perceptions of cybersecurity threats, which results in the better development of protective behaviors. Moreover, the result affirms the statement of Khan et al. (2024) that the college students are highly engaged in social media communication and learning, and this relationship is associated with their cybersecurity behaviors, including passwords and phishing awareness.

This result confirms to the Theory of Protection Motivation of Rogers (1975), which states that social media users who tend to encounter online risk or security warnings are probably to be urged to adopt safer habits of cybersecurity. The responsibility behind their behavior in the social platforms is dictated by their sensitivity to the dangers and their hope of being able to handle them. Also, the Theory of Planned Behavior (TPB) of Ajzen (1991, which states that the attitude towards behavior, norms sure and perceived behavioral control influence the

intention of a person predicting behavior. It can help to know how the attitude of the students towards cybersecurity, their perception of peer/social norms on social media, and their perceived capability to regulate the safe behavior of having a cybersecurity approach are the variables that encourage them to engage in the cybersecurity behavior.

CONCLUSION

First, it was revealed that social media engagement among students of Higher Education Institutions (HEIs) has a descriptive level of high, which is oftentimes observed. Therefore, students are often active on social media platforms. It was also revealed that cybersecurity behavior among students of Higher Education Institutions (HEIs) has a descriptive level of high, which is often observed. Therefore, students often practice responsible cybersecurity behaviors.

Second, this research showed that a significant relationship exists between social media engagement and cybersecurity behavior among college students, indicating a medium positive correlation.

Third, the findings support Protection Motivation Theory by Rogers (1975) which states that social media users who often face online risks or security alerts are likely to be encouraged to practice safer cybersecurity habits. Their awareness of potential threats and confidence in managing them determine how carefully they behave while using social platforms. Overall, the results indicate that social media engagement plays an important role in shaping responsible cybersecurity behavior among college students.

RECOMMENDATION

First, it is recommended that institutions may still encourage healthy and balanced social media engagement by strengthening good screen time usage habits among students of HEIs. Even though the indicators represent a high degree of responsible behavior, the students may also be helped to utilize structured programs that would promote the mindful use of technologies, including establishing a routine screen-time schedule, using phones less frequently at meals and before sleep, and managing notifications to avoid distractions. By combining digital well-being programs, time-management classes, and awareness, it might be possible to teach students to continue working productively offline and to keep positive and meaningful use of social media.

Second, it is recommended that Higher Education Institutions (HEIs) enhance the cybersecurity behavior of students by encouraging them to be more careful and responsible in their use of social media, particularly in addressing issues related to cyberbullying and hacking. To help allay the spread of fraudulent or incorrect information, students may be advised to ensure that the identity behind profile pictures is verified before accepting a friend request, control the sharing of personal details and real-time location, and carefully analyze the information online before reposting.

To deal with these anxieties, institution may use special programs like cybersecurity and anti-cyberbullying trainings and digital literacy, peer-support programs, and counseling solutions of victims of cyber bullying and hacking. By organizing, implementing, and sustaining awareness initiatives along with school-driven activities, the institutions may assist the students in being aware of online dangers, act accordingly in case of cyber threats, and establish responsible social media usage that can improve overall behavior in cybersecurity.

For future researchers studying the effect of social media engagement on cybersecurity behavior among students of HEIs, a simple and practical intervention could be recommended, including the short seminars or online courses with the emphasis on safe and responsible use of social media. Further research can be conducted on the efficacy of cybersecurity education, peer-led discussions, or interactive tasks that can show students how to protect their personal data, how to verify information on the Internet, and how to adjust privacy settings. A longitudinal or mixed-method study could also prove useful in establishing the presence of a program effect on the cybersecurity behavior of students in the long-term and give a better idea of how these programs can be effective in shaping the educational strategy.

REFERENCES

1. Adamczewska-Chmiel, K., Dudzic, K., Chmiela, T., & Gorzkowska, A. (2022). Smartphones, the epidemic of the 21st century: A possible source of addictions and neuropsychiatric consequences. International Journal of Environmental Research and Public Health, 19(9), 5152.
2. Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9), 5700.
3. Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. Technology in society, 73, 102258.
4. Arzmi, M. H. (2021). Scientific research misconducts: An overview. IIUM Journal of Orofacial and Health Sciences, 2(1), 1-3.
5. Bokoh, M. A., Bello, M. M., & Idowu, A. A. (2022). Use of social media platforms for dissemination of information and creating awareness about library resources and services among students in Lagos State University, Nigeria. Library Philosophy & Practice.
6. Bonisteel, I., Shulman, R., Newhook, L. A., Guttmann, A., Smith, S., & Chafe, R. (2021). Reconceptualizing recruitment in qualitative research. International Journal of Qualitative Methods, 20, 16094069211042493.
7. Brodowicz, M. (2024). Descriptive correlational design in research. Bhat, A. (2023). Descriptive correlational: Descriptive vs correlational research. Market Research: QuestionPro. https://www. questionpro. com/blog/descriptive-research-vs-correlational-research.
8. Cybersecurity Practices Among College Students: A Survey Study. In International Conference on MAchine inTelligence for Research & Innovations (pp. 147-159). Singapore: Springer Nature Singapore.
9. Davies, S. R., Wells, R., Zollo, F., & Roche, J. (2024). Unpacking social media'engagement': a practice theory approach to science on social media. Journal of Science Communication, 23(06).
10. Designing an Interactive Web-Based Social Media Platform for College Students. (2023). International Journal For Science Technology AndEngineering.
11. Hurley, M., & Tenny, S. (2023). Mean. In StatPearls [Internet]. StatPearls Publishing.
12. HWANG, H. J. (2023). The importance of anonymity and confidentiality for conducting survey research. Journal of Research and Publication Ethics, 4(1), 1-7.
13. Jadhav, D. S. (2024). Social media content consumption patterns by UG students in Shivaji University, Kolhapur Campus.
14. Jiang, Q., Chen, Z., Zhang, Z., & Zuo, C. (2023). Investigating links between Internet literacy, Internet use, and Internet addiction among Chinese youth and adolescents in the digital age. Frontiers in Psychiatry, 14, 1233303.
15. Journal of Philosophy, Culture & Political Science, 89(3). Davies, S. R.,Wells, R., Zollo, F., & Roche, J. (2024). Unpacking social media'engagement': a practice theory approach to science on social media. Journal of Science Communication, 23(06).
16. Karani, N. F., Sher, J., & Mophosho, M. (2022). The influence of screen time on children's language development: A scoping review. South African Journal of Communication Disorders, 69(1), 825.
17. Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Frontiers in Psychology, 11, 546546.
18. Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Frontiers in Psychology, 11, 546546.
19. Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Frontiers in Psychology, 11, 546546.
20. Khan, F., Arora, S., Pargaien, S., Pande, L., & Khati, K. (2023, September). Exploring the Relationship Between Digital Engagement and
21. Kotronoulas, G., & Papadopoulou, C. (2023). A primer to experimental and nonexperimental quantitative research: the example case of Tobacco-Related Mouth Cancer. Seminars in Oncology Nursing, 39(2), 151396.
22. Latih, R., & Zin, A. M. (2024). Cybersecurity behavior in the West Sumatra universities. JOIV: International Journal on Informatics Visualization, 8(3-2), 1976–1986.
23. Molina, S., & Eduardo, J. (2023b). Paradigms and different types of research. International Journal of Social Science and Human Research, 6(12).

24. Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decision Support Systems, 135, 113323.
25. Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decision Support Systems, 135, 113323.
26. Murdock, C. M., & Heidenreich, T. M. (2021). Mobile device usage across ages. Communication Complications.
27. Nguyen, L. T., & Tuamsuk, K. (2024). Unveiling scientific integrity in scholarly publications: a bibliometric approach. International Journal for Educational Integrity, 20, Article 16. DOI: 10.1007/s40979-024-00164-5.
28. Nguyen, T. D., Shih, M. H., Srivastava, D., Tirthapura, S., & Xu, B. (2021). Stratified random sampling from streaming and stored data. Distributed and Parallel Databases, 39(3), 665-710.
29. Ni, X., Shao, X., Geng, Y., Qu, R., Niu, G., & Wang, Y. (2020). Development of the social media engagement scale for adolescents. Frontiers in Psychology, 11, 701.
30. Nob[1], J. M. R., & Tañola, M. (2024). "Ang Magturo ay Di Biro": A Hermeneutic Phenomenological Study On The Lived-Experiences Of Math Educators In Out-Of-Field Teaching.
31. Nussipova, A. U., & Slanbekova, G. K. (2024). Social Media Landscape In The Republic Of Kazakhstan: Navigating Youth Behavior And Ensuring Information Security.
32. Obermayer, N., Kővári, E., Leinonen, J., Bak, G., & Valeri, M. (2022). How social media practices shape family business performance: The wine industry case study. European Management Journal, 40(3), 360–371.
33. Petropoulou, F. M., & Varouchas, E. (2024). Cracking the code: How social media and human behavior shape cybersecurity challenges. Human Factors in Cybersecurity, 127(127).*
34. Ruiz, A. P., & Cabigan, M. (2022). Social media engagement: Its relation to the psychosocial attributes of selected junior high school students. Social Media Engagement: Its Relation to the Psychosocial Attributes of Selected Junior High School Students, 104(1), 22.
35. Ruiz, a. p., & cabigan, m. (2022). social media engagement: its relation to the psychosocial attributes of selected junior high school students. social media engagement: its relation to the psychosocial attributes of selected junior high school students, 104(1), 22.
36. Sajikumar, S., & Ajithkumar, N. (2023). Understanding the emergence and significance of behavioral cybersecurity: A bibliometric analysis. Multidisciplinary Reviews, 6.
37. Schaltegger, T., Ambuehl, B., Bosshart, N., Bearth, A., & Ebert, N. (2025). Human behavior in cybersecurity: an opportunity for risk research. Journal of Risk Research, 1-12.
38. Stewart, L. (2025, February 11). Understanding informed consent in research. ATLAS.ti. https://atlasti.com/research-hub/informed-consent-in-research
39. Tabuga, A. D., Umlas, A. J. L., Zuluaga, K. M. C., & Domingo, S. N. (2023). How social networks influence access and utilization of weather and climate information: The case of upland farming communities in the Philippines. Philippine Institute for Development Studies Research Papers, 2023(3).
40. Titiakarawongse, C., & Boonkrong, S. (2023). A study of password management behaviors of young people. Applied Science and Engineering Progress, 16(4), 6580–6580.
41. Tran, M. N., Hogg, L., & Marshall, S. (2022). Understanding postgraduate students' perceptions of plagiarism: a case study of Vietnamese and local students in New Zealand. International Journal for Educational Integrity, 18(1),3.
42. Trepte, S., & Masur, P. K. (2023). Definitions of privacy. In The Routledge Handbook of Privacy and Social Media(pp. 3-15). Routledge.
43. Tsindos, T. (2023, March 21). Chapter 29: Recruitment and sampling. Qualitative Research – a Practical Guide for Health and Social Care Researchers and Practitioners. https://oercollective.caul.edu.au/qualitative-research/chapter/__unknown__-29/
44. VanBuren, J. M., Roalstad, S., Kay, M. T., Zuspan, S. J., Dean, J. M., & Brulotte, M. (2022). Development of a risk assessment and risk management tool for an academic research organization. Contemporary clinical trials, 119, 106812.

45. Weisburd, D., Britt, C., Wilson, D. B., & Wooditch, A. (2021). Measuring association for scaled data: Pearson's correlation coefficient. In Basic statistics in criminology and criminal justice (pp. 479-530). Cham: Springer International Publishing.
46. Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity vulnerability behavior scale in college during the COVID-19 pandemic. Jurnal Sisfokom (Sistem Informasi dan Komputer), 9(3), 395–399.*
47. Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity vulnerability behavior scale in college during the covid-19 pandemic. Jurnal