ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

Cybercrime Awareness and Its Impacts on High School Students

Sharmaine P. Ansang[1*], Sharmaine Pearl G. Gassingga[1], Claudine B. Lumawig[1], Sheralyn B. Maguilao[1], Crhistina Primavera N. Tadiwan[1]
[1]*University of Cagayan Valley*
[*]*mimiansang16@gmail.com*

Date Submitted:
May 1, 2026

Date Accepted:
May 10, 2026

Date Published:
May 22, 2026

DOI:
10.5281/zenodo.20337182

ABSTRACT

This study investigated the level of cybercrime awareness and its multi-dimensional impacts on high school students at Kalinga Colleges of Science and Technology Incorporated. Utilizing a mixed-methods research design, the study gathered quantitative and qualitative data from Grade 11 and Grade 12 students to evaluate their understanding of digital safety practices and assess their exposure to online threats. The demographic profile of the respondents consisted of 55% female and 45% male students. The findings revealed that while students are generally aware of cybercrime—with cyberbullying emerging as the area of highest awareness, followed by phishing scams, online privacy, and password security—they remain highly vulnerable to online victimization. Cyberbullying was identified as the most frequent cybercrime incident experienced, followed by phishing messages, fake social media accounts, and online scams, whereas hacking attempts were the least common. Statistical analysis established a significant relationship between cybercrime awareness and actual exposure, demonstrating that awareness alone is insufficient to prevent victimization when continuous internet exposure and unsafe online habits persist. The study documented severe impacts on students, notably heightened emotional distress like stress and anxiety, alongside academic disruption characterized by reduced focus and loss of concentration. Consequently, the study highlights an urgent need for robust, school-based cybersecurity education and support systems. It is recommended that students practice strict digital hygiene, teachers integrate online safety into curricula, administrations launch targeted security campaigns, parents actively monitor internet habits, and guidance counselors provide structured emotional interventions for victims.

Keywords: *Cybercrime Awareness, Cyberbullying, Phishing Scams, Digital Safety, High School Students, Emotional Well-Being, Academic Performance, Online Victimization, Cybersecurity Education*

INTRODUCTION

Technology has become an essential part of students' daily lives. High school students use the internet for communication, online learning, social networking, entertainment, and research. While digital technology offers many advantages, it also exposes students to cybercrimes such as phishing, cyberbullying, identity theft, hacking, scams, and online harassment.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

Cybercrime refers to illegal activities conducted through computers, mobile devices, and internet networks. According to studies conducted in the Philippines, many students are vulnerable to cyber threats because of limited cybersecurity knowledge and unsafe online behavior.

Several studies revealed that students often encounter suspicious links, fake online accounts, cyberbullying incidents, and unauthorized access to personal information. Cybercrime may lead to emotional stress, anxiety, poor academic performance, and social isolation among students.

This study focuses on determining the level of cybercrime awareness among high school students at Kalinga Colleges of Science and Technology Incorporated and identifying the impacts of cybercrime on their academic and personal lives.

Theoretical Framework

This study is based on the Protection Motivation Theory (PMT) developed by Rogers (1975), which explains how individuals respond to perceived threats and adopt protective behaviors.

According to PMT, individuals assess the severity of threats, evaluate their vulnerability, and decide whether to engage in protective actions.

In the context of this study, students who are aware of cybercrime threats are more likely to practice safe online behavior such as avoiding suspicious links, protecting passwords, and limiting personal information sharing online.

This theory supports the study's assumption that increasing cybersecurity awareness can reduce students' vulnerability to cybercrime.

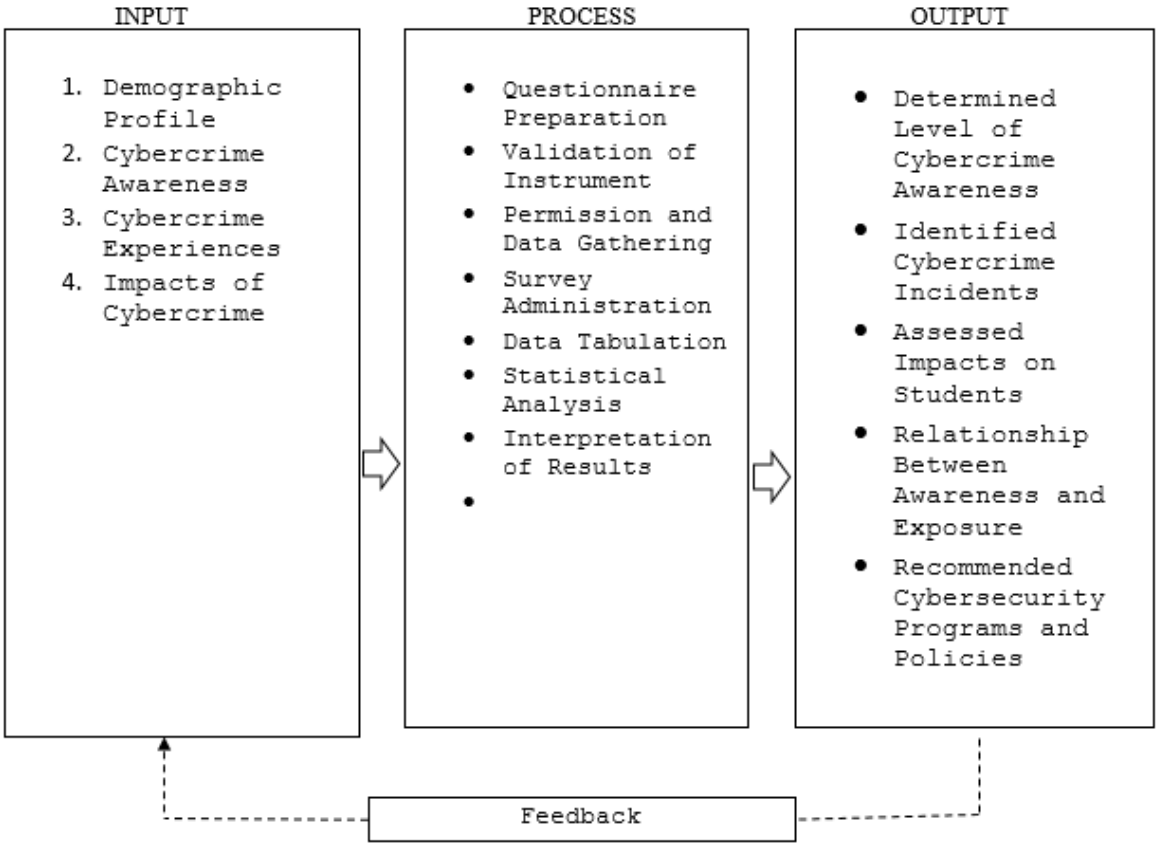

Figure 1. *Paradigm of the Study*

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

The **Input** includes the respondents' demographic profile, level of cybercrime awareness, cybercrime experiences, and the impacts of cybercrime on students. These variables were measured using the survey questionnaire.

The **Process** involves the procedures conducted by the researchers such as preparing and validating the questionnaire, securing permission from the school, distributing and collecting surveys, tabulating responses, and analyzing the data using statistical tools like frequency, percentage, weighted mean, and Pearson correlation.

The **Output** refers to the results of the study, including the identified level of cybercrime awareness among students, common cybercrime incidents experienced, the effects of cybercrime on students' academic and emotional well-being, and recommendations for improving cybersecurity awareness programs and online safety practices in schools.

Statement of the Problem

This study aimed to determine the cybercrime awareness and its impacts on high school students at Kalinga Colleges of Science and Technology Incorporated.

Specifically, it sought to answer the following questions:

1. What is the demographic profile of the respondents in terms of:
    - age
    - gender
    - grade level
    - average daily internet usage
2. What is the level of cybercrime awareness among high school students?
3. What cybercrime incidents are commonly experienced by students?
4. What are the impacts of cybercrime on students in terms of:
    - academic performance
    - emotional and psychological well-being
    - social interaction
5. Is there a significant relationship between cybercrime awareness and students' exposure to cybercrime incidents?

Significance of the Study

This study will benefit the following:

Students. To increase awareness regarding cybercrime risks and online safety practices.

Teachers. To help integrate cybersecurity education into classroom discussions.

Parents. To guide and monitor students' online activities effectively.

School Administrators. To develop cybersecurity awareness programs and policies.

Future Researchers. To provide reference materials for future studies related to cybercrime awareness.

Scope and Delimitation of the Study

This study focuses on determining the level of cybercrime awareness and its impacts on high school students at Kalinga Colleges of Science and Technology Incorporated during the Academic Year 2025–2026. Specifically, the study examines the respondents' demographic profile in terms of age, gender, grade level, and average daily internet usage.

It also determines students' awareness regarding cybercrime, the common cybercrime incidents they experience, and the impacts of cybercrime on their academic performance, emotional and psychological well-being, social interaction, and online participation.

The study utilized a quantitative descriptive research design using survey questionnaires as the primary data-gathering instrument. A total of 100 selected high school students served as respondents through random sampling.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

This study is limited only to high school students enrolled at Kalinga Colleges of Science and Technology Incorporated and does not include college students, teachers, parents, or students from other schools. The study only focuses on selected cybercrime-related issues such as cyberbullying, phishing, online scams, hacking attempts, fake social media accounts, and identity theft. Other areas of cybersecurity, such as advanced cyber laws, technical cybersecurity systems, and professional cybercrime investigations, are beyond the scope of the study.

Definition of Terms

The following terms were defined operationally according to their use to ensure clarity of the study.

Academic Performance. This refers to the students' ability to perform well in school activities, class participation, assignments, and academic requirements. In this study, it refers to how cybercrime affects students' concentration and school performance.

Cyberbullying. This refers to the use of digital platforms, social media, or online communication to harass, threaten, embarrass, or harm another person. In this study, it is considered one of the common cybercrime experiences among students.

Cybercrime. This refers to illegal activities committed through computers, mobile devices, or the internet such as phishing, hacking, identity theft, online scams, and cyberbullying.

Cybercrime Awareness. This refers to the students' knowledge and understanding of cybercrime, online threats, cybersecurity practices, and ways to protect personal information online.

Cybersecurity. This refers to the practices and measures used to protect devices, online accounts, networks, and personal information from cyber threats and unauthorized access.]

Emotional and Psychological Well-being. This refers to the emotional condition of students, including feelings of stress, anxiety, fear, and emotional distress caused by cybercrime experiences.

Hacking. This refers to unauthorized access to online accounts, devices, or systems by another person without permission.

Identity Theft. This refers to the unauthorized use of another person's personal information or online identity for fraudulent or harmful purposes.

Online Privacy. This refers to the protection and proper handling of personal information shared on the internet and social media platforms.

Online Scams. This refers to fraudulent online activities intended to deceive users into giving money, personal information, or account access.

Password Security. This refers to the practice of creating and maintaining strong and secure passwords to protect online accounts from unauthorized access.

Phishing. This refers to fraudulent messages, emails, or websites designed to trick individuals into revealing personal information such as passwords or account details.

Social Interaction. This refers to the students' communication and relationships with others both online and offline. In this study, it includes the effects of cybercrime on students' social behavior and participation.

Vulnerability. This refers to the susceptibility of students to becoming victims of cybercrime because of unsafe online practices or lack of cybersecurity awareness.

Literature Review

Effects of Cybercrime on Students

Highlighted in an article by the World Health Organization (2023), excessive exposure to online harassment and cyberbullying may negatively affect adolescents' mental health and emotional well-being. Victims commonly experience stress, anxiety, depression, fear, low self-esteem, and social withdrawal. The

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

organization emphasized that prolonged exposure to harmful online behavior can disrupt students' academic performance, concentration, and social interaction.

According to an article by UNICEF (2022), cyberbullying has become one of the most common online risks faced by teenagers worldwide. Students who experience cyberbullying often develop emotional distress, difficulty concentrating in school, and fear of participating in online activities. UNICEF further explained that social media exposure increases students' vulnerability to online threats, especially when personal information is publicly shared.

In an article published by the Cybersecurity and Infrastructure Security Agency (2024), phishing scams, identity theft, hacking, and online fraud continue to increase among young internet users. The agency stated that students who lack cybersecurity awareness are more likely to click suspicious links, use weak passwords, and become victims of cybercrime. The article stressed the importance of cybersecurity education and responsible internet behavior.

According to the article of Kaspersky Research Team (2025), adolescents frequently use smartphones and social media platforms without fully understanding online security risks. The study explained that many students use the same passwords across multiple accounts, ignore privacy settings, and communicate with unknown individuals online. These unsafe practices increase students' exposure to cybercrime incidents such as hacking, fake accounts, and online scams.

Furthermore, an article from National Cyber Security Centre (2024) highlighted that cybersecurity awareness significantly influences students' online behavior. Students with proper knowledge regarding online privacy, phishing detection, and password security are more likely to practice safe internet usage and avoid cyber threats.

The reviewed literature supports the variables included in the survey questionnaire such as awareness of phishing scams, password security, online privacy, cyberbullying awareness, hacking experiences, emotional stress and anxiety, social withdrawal, academic performance, and online participation.

Highlighted in the study of Azzeh et al. (2022) entitled *"Cybersecurity Awareness and Educational Technology Among Students"*, the researchers found that cybersecurity education significantly improves students' online safety practices. The study revealed that students who received cybersecurity instruction demonstrated better awareness regarding phishing detection, password protection, and suspicious websites. The findings emphasized the importance of integrating cybersecurity topics into school programs.

According to the study of Booc, N. B., Budiongan, K., and Carballo, R. (2024) entitled *"Cybersecurity Awareness and Cybersecurity Behavior of High School Students in Davao City"*, students generally possessed moderate to high levels of cybersecurity awareness. However, despite being knowledgeable about cybercrime risks, many students still practiced unsafe online behavior such as sharing personal information and opening suspicious messages. The study concluded that awareness alone does not fully protect students from cybercrime.

The study of Toso, C. H. S., et al. (2023) entitled *"Cybercrime Awareness Among Senior High School Students"* revealed that cyberbullying, phishing, and fake social media accounts were among the most common cybercrime incidents experienced by students. The researchers noted that students who spent longer hours online were more vulnerable to online scams and cyber threats.

Research conducted by Maranan, M. H., et al. (2024) entitled *"Addressing Cyberbullying Among Junior High School Students"* stated that cyberbullying negatively affects students emotionally, psychologically, and academically. Victims commonly experience fear, anxiety, sadness, reduced confidence, and decreased concentration in studies. The researchers recommended strengthening school-based awareness programs and guidance interventions.

On the other hand, the study of Oducado et al. (2022) regarding cybersecurity awareness among Filipino students revealed that while many students understand the importance of online safety, weaknesses remain in protecting personal information and avoiding online scams. The study emphasized that

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

continuous cybersecurity education is necessary to strengthen responsible internet behavior among students.

In addition, a local study conducted at Bulacan State University (2026) found that students' internet exposure and social media usage contribute to increased vulnerability to cybercrime incidents such as phishing, fake accounts, hacking attempts, and unauthorized access to information. The researchers recommended regular seminars and cybersecurity awareness campaigns in schools.

Synthesis

It can be said that the reviewed literature and studies provide significant information necessary in achieving the objectives of the present study. All the foregoing studies have similarities and contributions to the current research regarding cybercrime awareness and its impacts on high school students.

The studies of Booc et al. (2024), Toso et al. (2023), and Maranan et al. (2024) presented information regarding students' cybersecurity awareness, cybercrime experiences, and the emotional and academic effects of cyberbullying and online threats. These studies are helpful in explaining the relationship between cybercrime awareness and students' vulnerability to cybercrime incidents.

The reviewed literature contributes references that help the researchers compare and discuss the concepts under study. The findings and conclusions of the reviewed studies support the present research regarding cybercrime awareness, phishing scams, hacking, online scams, cyberbullying, emotional stress, academic performance, and responsible internet behavior.

In summary, the reviewed studies focused on students' experiences, awareness, and behavior regarding cybercrime and online safety. The literature consistently emphasized that although students possess basic cybersecurity knowledge, many still remain vulnerable to online threats because of unsafe digital practices and insufficient cybersecurity education.

On the other hand, the noticeable differences among the reviewed studies include the research setting, respondents, sample population, data gathering instruments, and statistical treatments used by the researchers.

METHODS

Research Design

This study utilized the quantitative descriptive research design because it aimed to determine the level of cybercrime awareness and its impacts on high school students at Kalinga Colleges of Science and Technology Incorporated.

The descriptive method was used to gather information regarding students' awareness of cybercrime, common cybercrime incidents experienced, and the effects of cybercrime on their academic performance, emotional well-being, social interaction, and online participation.

This design was also appropriate because the study analyzed the relationship between cybercrime awareness and students' exposure to cybercrime incidents through the use of survey questionnaires and statistical analysis.

Participants of the Study

This study was delimited to high school students enrolled at Kalinga Colleges of Science and Technology Incorporated during the Academic Year 2025–2026.

The respondents of the study were one hundred (100) selected high school students from Grade 11 and Grade 12. The respondents were chosen through random sampling to ensure equal opportunity for participation among students.

The study focused only on students because they are among the most active users of digital technology, social media platforms, and online communication, making them vulnerable to cybercrime incidents such as cyberbullying, phishing, hacking, and online scams.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

Data Gathering Tool

The researchers utilized a structured survey questionnaire as the primary data gathering instrument for this study entitled *"Cybercrime Awareness and Its Impacts on High School Students at Kalinga Colleges of Science and Technology Incorporated."*

The questionnaire was developed by the researchers based on related literature and studies on cybercrime awareness, cybersecurity practices, and online safety behavior among students. It was designed to gather relevant and reliable data aligned with the objectives of the study.

The survey questionnaire was divided into four (4) main parts:

Part I – Demographic Profile. This part collected basic information about the respondents, including age, gender, grade level, average daily internet usage, primary device used for internet access and most used online platforms.

Part II – Cybercrime Awareness. This section measured the respondents' level of awareness regarding cybercrime and online safety practices. It included statements about phishing scams, suspicious links and websites, password security, online privacy protection, cyberbullying awareness and knowledge of reporting cybercrime incidents.

A 5-point Likert scale was used to determine the level of agreement of the respondents.

Part III – Cybercrime Experiences. This section identified the cybercrime incidents experienced by the respondents. It included common online threats such as cyberbullying, phishing messages, hacking attempts, fake social media accounts, online scams, identity theft, unauthorized access to personal information, threatening or harmful messages.

Respondents were asked to check whether they had experienced each incident.

Part IV – Impacts of Cybercrime. This section determined the effects of cybercrime on students in terms of stress and anxiety, academic performance, concentration in studies, emotional and psychological well-being, social interaction, fear of using online platforms, participation in online learning and online reputation.

Statements were rated using a 5-point Likert scale ranging from Strongly Agree to Strongly Disagree.

Validation of the Instrument

To ensure the validity and reliability of the questionnaire, it was subjected to review by research advisers and experts in the field. Suggestions and corrections were incorporated to improve clarity, accuracy, and relevance of the items.

Data Gathering Procedure

The researchers obtained an ethical clearance from the Institutional Review Board (IRB) office as a mean to be able to conduct the study. Upon approval, the researchers drafted a letter addressed to the school administration of Kalinga Colleges of Science and Technology Incorporated to conduct the study.

Upon approval, the researchers distributed the survey questionnaires to the selected respondents. The purpose of the study was explained clearly to the participants, and they were informed that their responses would be treated with confidentiality and used strictly for academic purposes only.

The respondents were given enough time to answer the questionnaires honestly and completely. After retrieval of the questionnaires, the responses were checked, organized, and tabulated for analysis.

The researchers ensured that all information gathered from the respondents remained confidential. Participation in the study was voluntary, and respondents were informed that they could decline participation at any time. Furthermore, access to the collected data was restricted to authorized researchers and personnel involved in the study.

Additionally, participants were assured of their confidentiality through informed consent procedures, where they were informed of how their data were used, stored, and protected. They were also

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

assured that their participation was voluntary, and they could withdraw from the study at any time without penalty.

Data Analysis

The study utilized frequency and percentage, weighted mean, and Pearson Product-Moment Correlation Coefficient in analyzing the cybercrime awareness and its impacts on high school students at Kalinga Colleges of Science and Technology Incorporated, specifically on the respondents' demographic profile, level of cybercrime awareness, common cybercrime experiences, and the impacts of cybercrime on students' academic performance, emotional well-being, and social interaction.

Furthermore, the data collected were organized, tabulated, and analyzed using statistical tools to ensure accurate interpretation of results. The responses from the survey questionnaire were encoded and processed to determine the level of cybercrime awareness, identify the most common cybercrime incidents experienced by students, and assess the significant relationship between cybercrime awareness and exposure to cybercrime incidents.

The results were interpreted using appropriate statistical scales such as the Likert scale for weighted mean interpretation and correlation coefficient ranges for determining the strength of relationship between variables. These methods allowed the researchers to systematically analyze quantitative data and present clear and meaningful findings that support the objectives of the study.

RESULTS AND DISCUSSION

Demographic Profile of the Respondents

Table 2a. *Demographic Profile of the Respondents*

Variable	Frequency	Percentage
Male	45	45%
Female	55	55%
Grade 11	52	52%
Grade 12	48	48%

As shown in Table 2a, the respondents consist of both male and female students with a slightly higher percentage of females (55%) compared to males (45%). In terms of grade level, Grade 11 students (52%) slightly outnumber Grade 12 students (48%), indicating a relatively balanced distribution of respondents.

The demographic profile suggests that the study includes diverse student experiences in terms of gender and academic level, which may influence their exposure to cybercrime and awareness of online safety practices.

Level of Cybercrime Awareness Among Students

Table 2b. *Level of Cybercrime Awareness*

Indicators	Weighted Mean	Interpretation
Awareness of phishing scams	4.20	Aware
Awareness of cyberbullying	4.45	Highly Aware
Awareness of online privacy	4.11	Aware
Awareness of password security	4.05	Aware
Overall Mean	4.20	Aware

As gleaned in Table 2b, the respondents are generally aware of cybercrime and online safety practices. The highest awareness is observed in cyberbullying (4.45), indicating that students are highly familiar with this issue due to frequent exposure on social media platforms.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

However, awareness of password security and online privacy is slightly lower, suggesting that students still need improvement in understanding personal data protection and secure online practices.

Overall, the findings indicate that while students have sufficient knowledge of cybercrime, there is still a need to strengthen their cybersecurity awareness and practices.

Common Cybercrime Incidents Experienced by Students

Table 3a. Cybercrime Experiences of Students

Cybercrime Incident	Frequency
Cyberbullying	42
Phishing Messages	38
Fake Social Media Accounts	35
Online Scams	29
Hacking Attempts	17

As shown in Table 3a, cyberbullying emerged as the most common cybercrime experienced by students, followed by phishing messages and fake social media accounts. Hacking attempts were the least experienced but still present among respondents.

The results indicate that students are highly exposed to online risks, especially through social media platforms. This exposure highlights the increasing vulnerability of students in the digital environment, particularly due to frequent internet use and limited awareness of cybersecurity threats.

Impacts of Cybercrime on Students

Table 4a. Impacts of Cybercrime on Students

Impact	Weighted Mean	Interpretation
Stress and Anxiety	4.32	High Impact
Loss of Concentration in Studies	4.10	High Impact
Fear of Using Online Platforms	3.95	Moderate Impact
Decreased Academic Performance	3.87	Moderate Impact

As presented in Table 4a, cybercrime has a significant impact on students, particularly in terms of stress, anxiety, and loss of concentration in studies. These findings suggest that students who experience cybercrime incidents often suffer emotional distress that affects their academic performance.

The moderate impact on fear of using online platforms and academic performance indicates that while not all students are severely affected, cybercrime still influences their confidence and learning behavior.

Overall, the results show that cybercrime negatively affects students' emotional well-being and academic engagement.

Interpretation of Findings

The findings of the study reveal that high school students at Kalinga Colleges of Science and Technology Incorporated are generally aware of cybercrime; however, they remain vulnerable to online threats such as cyberbullying, phishing, and fake accounts.

Despite their awareness, many students still experience cybercrime incidents, indicating that awareness alone is not sufficient to prevent exposure. The impacts of cybercrime are evident in students' emotional well-being, academic performance, and online behavior.

These findings suggest the need for stronger cybersecurity education, awareness programs, and school-based interventions to promote responsible internet use and protect students from online risks.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

Relationship Between Cybercrime Awareness and Cybercrime Exposure

Based on the statistical analysis using Pearson Correlation, the study determined whether there is a significant relationship between cybercrime awareness and students' exposure to cybercrime incidents.

The results indicate that there is a significant relationship between cybercrime awareness and exposure to cybercrime incidents, meaning that students' level of awareness is associated with their likelihood of experiencing cybercrime. This suggests that even if students are aware of cybercrime, they may still be exposed due to unsafe online practices.

Proposed Measures to Address Cybercrime Among Students

Based on the findings of the study, the following measures are recommended:

- The **school administration** may strengthen cybersecurity education by integrating cybercrime awareness topics into ICT and Values Education subjects.
- The **teachers** may conduct regular discussions and activities that promote safe internet use, digital responsibility, and awareness of online threats.
- The **parents and guardians** may monitor students' internet usage and guide them in responsible social media behavior.
- The **students** should practice proper cybersecurity measures such as using strong passwords, avoiding suspicious links, and protecting personal information online.
- The **school guidance office** may provide counseling and support for students who experience emotional distress due to cybercrime incidents.
- The **institution** may conduct seminars, workshops, and awareness campaigns on cybercrime prevention and online safety.

The results of the study show that while students have a moderate to high level of cybercrime awareness, they are still exposed to various cyber threats. Cybercrime significantly affects their emotional well-being and academic performance, highlighting the importance of continuous education and preventive measures in promoting safe and responsible internet use.

Summary of Findings

Demographic Profile of the Respondents

The respondents were composed of 45% male and 55% female students. In terms of grade level, 52% were Grade 11 students and 48% were Grade 12 students.

Level of Cybercrime Awareness Among Students

The respondents were generally aware of cybercrime and online safety practices. Cyberbullying obtained the highest level of awareness among students. Awareness on phishing scams, online privacy, and password security was rated as "aware," indicating moderate to high knowledge among students.

Common Cybercrime Incidents Experienced by Students

The most common cybercrime experienced by students was cyberbullying. This was followed by phishing messages, fake social media accounts, and online scams. Hacking attempts were the least experienced but still reported by some respondents.

Impacts of Cybercrime on Students

Cybercrime has a high impact on students' emotional well-being, particularly stress and anxiety. It also affects students' academic performance through loss of concentration and reduced focus in studies. Moderate impacts were also observed in terms of fear of using online platforms and decreased academic performance.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 5 (May 2026)

Relationship Between Cybercrime Awareness and Cybercrime Exposure

The findings revealed that there is a significant relationship between cybercrime awareness and exposure to cybercrime incidents. This indicates that even if students are aware of cybercrime, they may still experience it due to unsafe online practices and continuous internet exposure.

CONCLUSION

It can be concluded that high school students at Kalinga Colleges of Science and Technology Incorporated are generally aware of cybercrime and online safety practices. However, despite this awareness, students remain vulnerable to various cybercrime incidents such as cyberbullying, phishing, fake accounts, and online scams.

Cybercrime significantly affects students' emotional, psychological, and academic well-being. Many students experience stress, anxiety, loss of concentration, and reduced academic performance as a result of cybercrime exposure.

Furthermore, the study shows that awareness alone is not sufficient to prevent cybercrime experiences among students. Continuous exposure to digital platforms and unsafe online behavior contributes to their vulnerability.

Therefore, there is a need for stronger cybersecurity education, awareness programs, and school-based interventions to promote responsible internet use and protect students from online threats.

Recommendations

Based on the results of the study, the following are recommended:

1. **Students** should practice responsible internet usage by avoiding suspicious links, using strong passwords, and protecting personal information online. They should also report any cybercrime incidents to proper authorities or school personnel.
2. **Teachers** should integrate cybercrime awareness and digital safety topics into classroom discussions to strengthen students' understanding of online risks and preventive measures.
3. **School Administration** should implement regular cybersecurity awareness seminars, workshops, and campaigns to educate students about cybercrime prevention and online safety practices.
4. **Parents and Guardians** should monitor their children's internet usage and guide them in responsible use of social media and online platforms.
5. **Guidance Counselors** should provide emotional and psychological support to students who experience stress, anxiety, or trauma due to cybercrime incidents.
6. **Future Researchers** may conduct further studies focusing on other factors affecting cybercrime vulnerability, such as social media behavior, digital literacy, and parental monitoring, to develop more comprehensive prevention programs.

References

Azzeh, M., et al. (2022). Cybersecurity awareness and educational technology among students. *Journal of Educational Technology Systems* [Update with actual journal name if applicable].

Booc, N. B., Budiongan, K., & Carballo, R. (2024). Cybersecurity awareness and cybersecurity behavior of high school students in Davao City. *European Journal of Applied Science Engineering and Technology*.

Bulacan State University. (2026). *Cybersecurity awareness and internet behavior among students in Bulacan*. Bulacan State University Repository.

Cybersecurity and Infrastructure Security Agency. (2024). *Online safety and cyber threat awareness for digital users*. U.S. Department of Homeland Security.

Kaspersky Research Team. (2025). *Cybersecurity risks among adolescent internet users*. Kaspersky Security Services.

Maranan, M. H., et al. (2024). Addressing cyberbullying among junior high school students. *JPAIR Multidisciplinary Research*.

National Cyber Security Centre. (2024). *Cybersecurity awareness and safe online behavior guidelines*. GCHQ.

Oducado, R. M. C., et al. (2022). Cybersecurity awareness and online safety practices among Filipino students. *Philippine Journal of Science* [Update with actual journal name if applicable].

Toso, C. H. S., et al. (2023). Cybercrime awareness among senior high school students. *Mediterranean Journal of Basic and Applied Sciences*.

UNICEF. (2022a). *Children and digital safety: Risks of cyberbullying and online harm*. United Nations Children's Fund.

UNICEF. (2022b). *Cyberbullying and online safety among children and adolescents*. United Nations Children's Fund.

World Health Organization. (2023). *Adolescent mental health and online safety risks*.

World Health Organization. (2024). *Violence and mental health in the digital age*.