

Self-Reported Cybersecurity Competency Of Criminology Students In The Second District Of North Cotabato

April Dianne C. Lapis¹  | John Earl T. Amang²  | Romelyn V. Pezana³  | Reynan G. Tarife⁴  | Jessa Mae Acuas⁵ 
 | Rico O. Soledad⁶ 

¹⁻⁵ Central Mindanao Colleges,
Kidapawan City, Philippines

Abstract

Introduction: The increasing prevalence of cyber threats, including identity theft, online fraud, and data breaches, highlights the need for cybersecurity education among criminology students, who are future professionals in crime prevention and digital investigations. However, limited evidence describes students' cybersecurity competency and whether it varies across educational and technology-related factors.

Objective: This study aimed to determine the level of self-reported cybersecurity practices among incoming fourth-year criminology students and examine differences according to school, primary device used, and preferred social media platform.

Methods: A cross-sectional descriptive-comparative design was employed among 298 incoming fourth-year criminology students with prior cybersecurity exposure from Central Mindanao Colleges, Colegio de Kidapawan, and Makilala Institute of Science and Technology in the Second District of North Cotabato, Philippines. Data were collected using an adapted self-report Cybersecurity Competency Scale. Descriptive statistics and Kruskal–Wallis tests were used to analyze the data.

Results: Participants reported a very high level of self-reported cybersecurity practices ($M = 4.38$, $SD = 0.75$). No statistically significant differences were found according to school, primary device used, or preferred social media platform (all $p > .05$). However, subgroup sizes were highly unequal, and the findings were based solely on self-reported data.

Conclusions: The findings indicate high self-reported cybersecurity engagement among the selected criminology students, with no significant differences across the examined factors. Although interpreted through Protection Motivation Theory and the Technology Acceptance Model, these theoretical constructs were not directly measured. The findings support sustained, inclusive, and practice-oriented cybersecurity education. Future studies should incorporate objective, performance-based assessments and more balanced samples to determine whether self-reported competency corresponds with actual cybersecurity knowledge and skills.

Correspondence

April Dianne C. Lapis, Central
Mindanao Colleges,
Philippines
Email: alapis@cmc.edu.ph

Keywords: Self-Reported Cybersecurity Competency; Criminology Students; Digital Safety Practices; Cybercrime Prevention; Higher Education; Philippines

Cite as: Lapis, A. D. C., Amang, J. E. T., Pezana, R. V., Tarife, R. G., Acuas, J. M., & Soledad, R. O. (2026). Self-reported cybersecurity competency of criminology students in the Second District of North Cotabato. *Review of Studies on Criminology, Sociology, and Law*, 1–17. <https://doi.org/10.68354/742139>



© The Author(s) 2026. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License.

1. Introduction

In the contemporary digital environment, cyber threats such as identity theft, online fraud, phishing attacks, and data breaches have become increasingly prevalent. This growing concern necessitates heightened awareness among college students, particularly those enrolled in criminology programs, whose future professional roles involve crime prevention and investigation in both physical and digital domains. In international contexts, studies of undergraduate students report that a substantial proportion have experienced cyberattacks, with phishing the most prevalent, highlighting the urgent need to strengthen cybersecurity education (Hazarika, 2025). As students advance in their academic training, developing skills to identify cyber risks and implement protective measures becomes crucial (CNNIC, 2022).

The relationship between students' level of cybersecurity knowledge and the extent of their academic exposure to cybersecurity concepts is a crucial area of inquiry. The quality, depth, and integration of cybersecurity education within the curriculum largely shape awareness and preparedness against cyber threats. Despite the global expansion of internet usage, with over 4.7 billion users worldwide, many students remain inadequately informed about cyber risks because they have limited participation in formal cybersecurity training (Alharbi & Tassaddiq, 2021). This knowledge deficiency may have serious implications, especially given the projected global cost of cybercrime, which is projected to exceed US\$10.5 trillion annually by 2025 (Morgan, 2020). Therefore, strengthening cybersecurity education is imperative not only for personal protection but also for equipping future criminology professionals with the competencies needed to address cyber-related offenses. For clarity, this study follows the distinction commonly drawn in the literature among cybersecurity awareness (recognition of risks), knowledge (factual understanding), perceived competency (self-assessed ability), protective behavior (reported actions), and actual performance (objectively demonstrated skill); the present study measures self-reported perceived competency and protective behavior, not objectively demonstrated performance.

Within the Philippine context, internet utilization among college students continues to expand for academic, social, and communicative purposes. However, this increased reliance on digital platforms is not always matched with adequate cybersecurity awareness and practical defensive skills. As a result, students remain vulnerable to cyber threats, which may compromise personal data and pose broader security risks to educational institutions and local communities. Existing academic programs may not sufficiently address real-world cybersecurity challenges, particularly in developing applied skills relevant to crime prevention and digital forensics (Dapitan et al., 2024).

Specifically, this study focuses on the Second Legislative District of the Province of Cotabato (North Cotabato), a political and administrative subdivision in Region XII (SOCCSKSARGEN), Philippines. The Second District comprises several municipalities, including Kidapawan City, Makilala, M'lang, Tulunan, Magpet, Antipas, and President Roxas, among others, which are characterized by a mix of urban and rural communities. Within this district, the study purposively selected three higher education institutions offering criminology programs: Central Mindanao Colleges (CMC), located in Kidapawan City; Colegio de Kidapawan (CDK); and Makilala Institute of Science and Technology (MIST), in Makilala. These institutions were chosen because they represent key providers of criminology education within the district and collectively reflect the academic environment and student population of criminology learners in this geographical area. Clarifying this scope helps readers unfamiliar with the Philippine local government structure better understand the study's setting and the rationale for participant selection.

Despite the growing relevance of cybersecurity in criminology education, a research gap remains regarding how criminology students in North Cotabato perceive their own cybersecurity knowledge and preparedness. To date, no published study has examined this population specifically within the Second District, and the district's mixed urban–rural composition and multiple criminology-granting institutions give the setting practical, context-specific value for curriculum planning, even though a geographic

absence of prior research is, on its own, only a modest justification for originality. Cybersecurity knowledge frameworks such as Catal et al. (2023) inform how the construct is operationalized here, although that work does not document the local research gap. Addressing this gap is essential to develop context-specific educational interventions and enhance curriculum design tailored to local needs. This study was guided by the following research questions: (1) What is the level of criminology students' self-reported cybersecurity competency across the instrument's dimensions? (2) Does self-reported cybersecurity competency differ by school? (3) Does it differ by primary device used? (4) Does it differ by preferred social media platform?

This study is anchored in Sustainable Development Goal (SDG) 4: Quality Education, evaluating whether criminology students have the essential cybersecurity knowledge and skills needed to meet the demands of the digital age. It also supports SDG 16: Peace, Justice, and Strong Institutions by preparing future law enforcement and criminology professionals to address cybercrime and promote digital safety in their communities. This study uses Protection Motivation Theory and the Technology Acceptance Model as interpretive lenses for discussing the findings; because the questionnaire does not operationalize their constructs (e.g., perceived severity, response efficacy, perceived usefulness), the study does not directly test either theory.

This research is expected to improve cybersecurity education by emphasizing the integration of practical, skills-based learning into criminology curricula. Moreover, the study offers both academic and social significance by promoting cybersecurity awareness and responsible digital behavior among students. The results will be disseminated through academic publications, conferences, seminars, and institutional collaborations to inform policy development and curriculum enhancement at both local and national levels. Ultimately, this research aims to foster a more cybersecurity-aware and resilient academic community within the Second District of North Cotabato.

2. Materials and Methods

2.1. Respondents and Sampling Procedure

The study respondents comprised 298 incoming fourth-year criminology students enrolled during the first semester of the 2025–2026 academic year at higher education institutions within the Second District of North Cotabato. The study employed a cross-sectional descriptive-comparative survey design to determine and compare the respondents' cybersecurity competency based on the variables identified in the study. The respondents were selected based on the following inclusion criteria: (1) they were officially enrolled in an undergraduate criminology program as incoming fourth-year students during the first semester of the 2025–2026 academic year; and (2) they had prior exposure to cybersecurity concepts through coursework, institutional seminars or webinars, training programs, or other related learning activities. Confirmed prior cybersecurity exposure through student self-report at the time of recruitment. It excluded students who were not enrolled during the specified period or who had no prior exposure to cybersecurity concepts. The selection of incoming fourth-year students was intended to focus on learners who had already completed substantial coursework in criminology and were approaching their final year of study. However, because respondents were surveyed during the first semester, before completing their final-year coursework, their cybersecurity competency may not yet reflect the full range of competencies they could develop during their remaining academic requirements.

Moreover, the requirement of prior cybersecurity exposure should be recognized as a methodological limitation. While this criterion ensured that the respondents had sufficient background to assess cybersecurity-related competencies, it may have introduced selection bias by excluding students with little or no prior exposure to cybersecurity. Consequently, the observed level of competency may be higher than what would be obtained from the broader population of incoming fourth-year criminology students. The findings should therefore be interpreted as applicable specifically to the 298 incoming fourth-year criminology students who met the study's inclusion criteria, particularly those with prior exposure to cybersecurity concepts, rather than generalized to all incoming fourth-year criminology students without qualification.

By focusing on this population, the study aims to examine the relationship between criminology students' existing cybersecurity competencies and their preparedness for professional roles in law enforcement and digital crime prevention—areas in which such knowledge is increasingly critical. This approach mitigates the potential limitation of including students who have not yet completed their fourth-year curriculum by ensuring that all respondents have foundational exposure to the competencies under investigation.

In this study, the researchers used proportionate stratified convenience sampling by school to ensure that the three participating higher education institutions—Central Mindanao Colleges (CMC), Makilala Institute of Science and Technology (MIST), and Colegio de Kidapawan (CDK)—were proportionally represented. The researchers first divided the eligible population into three strata by school affiliation. Based on the number of eligible incoming fourth-year criminology students in each institution, the researchers determined the corresponding proportion of respondents to be included in the study.

Using proportionate allocation, the researchers selected a total of 298 respondents from the three institutions. CMC contributed 130 respondents, MIST contributed 100 respondents, and CDK contributed 68 respondents, resulting in a total sample of 298 incoming fourth-year criminology students.

Table 1. Proportionate Allocation of Respondents by Higher Education Institution

Higher Education Institution	Eligible Student Population	Proportion	Allocated Respondents
Central Mindanao Colleges (CMC)	195	43.62%	130
Makilala Institute of Science and Technology (MIST)	150	33.56%	100
Colegio de Kidapawan (CDK)	102	22.82%	68
Total	447	100.00%	298

Note. The allocation was determined using the proportionate sampling formula:

$$n_i = (N_i / N) \times n$$

Where n_i represents the required sample from each institution, N_i represents the eligible population of the institution, N represents the total eligible population, and n represents the overall target sample of 298 respondents.

After determining the number of respondents required from each institution, the researchers recruited participants who met the established inclusion criteria, particularly those who were officially enrolled as incoming fourth-year criminology students during the first semester of the 2025–2026 academic year and had prior exposure to cybersecurity concepts through coursework, seminars, webinars, training, or related learning activities.

Although the number of respondents from each institution was determined proportionately, participants within each stratum were selected through convenience sampling. Thus, the procedure is more accurately described as proportionate stratified convenience sampling rather than stratified random sampling (Cleland et al., 2023). This approach ensured representation from CMC, MIST, and CDK while recognizing that respondents within each institution were not selected through random procedures. Consequently, interpret the findings primarily within the context of the participating institutions and respondents who met the study's inclusion criteria, and generalize to all incoming fourth-year criminology students with caution.

2.2. Research Instruments

The study employed a structured questionnaire adapted from the Cyber Security Competency Scale developed by Santhosh and Thiyagu (2024). The original scale was developed to assess cybersecurity competency among prospective teachers and was grounded in a review of existing digital

competence and digital safety frameworks, including the works of Calvani et al. (2008), Cartelli (2010), Falloon (2020), Janssen et al. (2013), Redecker (2017), Skov (2016), Punie and Tomczyk (2019), Tretinjak and Anđelić (2016), and Vuorikari et al. (2016). The original instrument initially consisted of 113 items covering 12 dimensions of cybersecurity. Following expert evaluation, 21 items were modified, and 13 items were deleted. The resulting draft instrument contained 93 items organized into nine dimensions of cybersecurity competency. These dimensions were: (1) Social Networking Safety and Security, (2) Dealing with Fake Information, (3) Mobile Phone Security and Safety, (4) Email and Password Security and Safety, (5) Managing Digital Footprint, (6) Online Privacy and Wi-Fi Safety, (7) Apps Safety and Security, (8) Web Conferencing Safety, and (9) Digital Learning Resource Safety, Plagiarism, and Copyright Infringement.

The original 93-item scale consisted of 79 positively worded items and 14 negatively worded items. The instrument used a three-response format consisting of Yes, No, and Unsure, with differential scoring for positive and negative statements. In the item analysis conducted by Santhosh and Thiyagu (2024), 15 items were removed based on item-level analysis, resulting in a final 78-item scale consisting of 72 positive items and six negative items. The final scale demonstrated a Cronbach's alpha of .906 and a split-half correlation coefficient of .851, indicating strong internal consistency and reliability. For the present study, the instrument was adapted from the final structure of the Santhosh and Thiyagu (2024) scale to make the items appropriate for incoming fourth-year criminology students. The adaptation focused on contextualizing the wording and examples to the respondents' academic background and the cybersecurity situations they may encounter in criminology-related learning and professional environments. Items that remained conceptually relevant to criminology students were retained, while wording that specifically referred to prospective teachers or teacher-oriented contexts was revised to reflect the target population.

The adapted questionnaire retained the nine cybersecurity competency dimensions of the original scale as its principal content domains. These were Social Networking Safety and Security, Dealing with Fake Information, Mobile Phone Security and Safety, Email and Password Security and Safety, Managing Digital Footprint, Online Privacy and Wi-Fi Safety, Apps Safety and Security, Web Conferencing Safety, and Digital Learning Resource Safety, Plagiarism, and Copyright Infringement. This structure is consistent with the original instrument and provides a clear basis for measuring cybersecurity competency among criminology students. The adaptation did not directly replicate the original scale because the respondents, educational context, and intended application differed from those of the original instrument. Accordingly, the present study treated the questionnaire as an adapted research instrument and evaluated its psychometric properties in the context of the current respondents rather than assuming them solely from the reliability evidence reported by Santhosh and Thiyagu (2024).

Before administering the final questionnaire, the adapted instrument underwent expert review to determine whether the revised items were appropriate for criminology students. The evaluation focused on the relevance, clarity, appropriateness, and alignment of the items with the intended cybersecurity competency domains. The experts' recommendations informed revisions to the wording and contextual appropriateness of the items before pilot administration. The adaptation process also ensured that the original meaning of the cybersecurity competency domains was preserved. Changes therefore focused primarily on contextualizing the items for criminology students rather than introducing unrelated constructs. This approach maintained conceptual continuity with the Santhosh and Thiyagu (2024) instrument while allowing the questionnaire to reflect the educational and disciplinary context of the present study. Before the main data collection, the adapted questionnaire was pilot-tested with 30 students who had characteristics comparable to those of the target respondents but were not included in the final study sample. The pilot test assessed the clarity of the adapted items and provided preliminary evidence of internal consistency.

The pilot test produced a Cronbach's alpha of .87 for the overall adapted instrument, indicating good internal consistency. The reliability coefficients for the two broad analytical groupings used in the present study were .83 for cybersecurity knowledge and .85 for cybersecurity competency. These

coefficients exceeded the commonly accepted .70 threshold for research instruments and indicate satisfactory internal consistency (Nunnally & Bernstein, 1994). The two broad groupings used in the present study should not be confused with the nine dimensions of the original Santhosh and Thiyagu (2024) scale. The nine dimensions represent the specific cybersecurity competency domains retained from the source instrument, whereas the two groupings represent the broader analytical categorization adopted by the present study. Thus, the nine domains serve as the detailed content areas through which the broader cybersecurity constructs were assessed. Given the relatively small pilot sample of 30 participants, the pilot reliability coefficients were treated as preliminary evidence of internal consistency rather than as definitive evidence of the psychometric adequacy of the adapted instrument. The reliability of the instrument was therefore considered alongside the expert review and the results from the final administration.

Using an adapted instrument also requires interpreting the findings in the context of criminology students. Although Santhosh and Thiyagu (2024) established strong reliability for the original 78-item scale, with a Cronbach's alpha of .906 and a split-half correlation of .851, these values cannot automatically be transferred to the present population because the instrument was modified and administered to a different group of learners. The present study's reliability results therefore provide more direct evidence of the adapted questionnaire's internal consistency for the current sample.

The structured questionnaire utilized a five-point Likert-type scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). For data analysis, the mean scores were interpreted using predetermined intervals, wherein a mean of 4.20–5.00 indicated a Very High level, suggesting a strong positive response and a high level of the self-reported cybersecurity practice measured; 3.40–4.19 indicated a High level, reflecting a positive but less pronounced response; 2.60–3.39 indicated a Moderate level, suggesting a neutral or mixed response and an average self-reported level of the practice; 1.80–2.59 indicated a Low level, reflecting a low self-reported level of the practice; and 1.00–1.79 indicated a Very Low level, indicating a minimal self-reported level of the practice measured.

2.4. Data Analysis

The researchers employed specific statistical tools to analyze the data and answer the research questions. The mean was used to determine the average level of perceived cybersecurity awareness among college students. This involved summing all individual responses and dividing the total by the number of participants, providing a measure of the typical level of awareness within the sample. The standard deviation quantified how much responses varied around the mean. A high standard deviation indicated a wide variation in students' awareness levels, while a low standard deviation suggested that most students reported similar levels of perceived cybersecurity awareness. The researchers used the updated IBM SPSS Statistics software to analyze the data. Although the researchers initially considered a One-Way Analysis of Variance (ANOVA), the data did not meet the normality assumption. Consequently, the Kruskal–Wallis H test was employed as a nonparametric alternative to determine whether significant differences existed in perceived cybersecurity awareness across three or more independent groups.

The Kruskal–Wallis test was appropriate because the comparison groups were independent and the dependent variable was an aggregated multi-item score that did not meet the normality assumption required for parametric analysis. The test allowed the researchers to compare distributions of cybersecurity awareness scores across demographic groups without requiring normally distributed data. The analysis was performed using IBM SPSS Statistics, with the level of significance set at 0.05. For each comparison, the results were interpreted based on the Kruskal–Wallis H statistic, degrees of freedom, and p-value. Descriptive results, including the median, interquartile range, and mean rank, were considered in interpreting the distribution of scores across groups. Where appropriate, the researchers also considered an effect-size estimate to determine the magnitude of observed group differences. A significant result ($p < .05$) indicates that at least one group differs significantly from the others, whereas a nonsignificant result ($p \geq .05$) indicates that a statistically detectable difference among the groups was not established in the sample. The Kruskal–Wallis test was therefore used to more appropriately

compare cybersecurity awareness across demographic categories under the observed distributional conditions.

2.5 Ethical Considerations

Before data collection, the study protocol, including the questionnaire and informed-consent materials, was submitted to the institution's Research Ethics Committee (Central Mindanao Colleges) for review and approved under Protocol No. ERC-2025-CRIM-0016 on September 12, 2024. Participation was voluntary; students were informed of the study's purpose, procedures, and their right to decline or withdraw at any time without penalty, and we obtained written or electronic informed consent before administering the questionnaire. The researchers collected and stored responses without directly identifying information, and limited access to the dataset to the research team; the researchers will retain and dispose of the data in accordance with institutional data-protection policy. The researchers obtained permission to conduct the study from the administration of each participating institution (CMC, CDK, and MIST). All respondents were of legal age, with no minors involved, and their respective institutions provided informed consent before voluntary participation in the survey.

3. Results and Discussion

The demographic profile of respondents provides valuable insight into the cybersecurity competency of criminology students in the Second District of North Cotabato.

Table 2. Frequency Distribution of Participant Demographics (N = 298)

Variable	Category	<i>n</i>	%
School	CMC	165	55.4
	MIST	83	27.9
	CDK	50	16.8
	Total	298	100.0
Primary Device Used	Mobile Phone	291	97.7
	Laptop	3	1.0
	Personal Computer	3	1.0
	Total	297	99.7
Preferred Social Media	Facebook	261	87.6
	TikTok	23	7.7
	Instagram	10	3.4
	X (Twitter)	2	0.7
	YouTube	2	0.7
	Total	298	100.1*

Table 2 presents the frequency distribution of participants' demographic characteristics by school affiliation, daily device use, and preferred social media platforms. Regarding school affiliation, most respondents are from Central Mindanao Colleges (CMC), accounting for 55.4% of the total sample. This is followed by students from MIST (27.9%) and CDK (16.8%). The dominance of respondents from CMC suggests that the findings largely reflect the digital practices and experiences of students from this institution. However, including participants from MIST and CDK still allows for a broader institutional perspective. Previous studies indicate that institutional context, including access to

digital infrastructure and exposure to technology-related training, can influence students' digital behavior and competencies (Bendler & Felderer, 2023).

Regarding the primary device used, the data reveal an overwhelming reliance on mobile phones: 97.7% of respondents reported that smartphones are their primary device. In contrast, only 1.0% reported using laptops and another 1.0% reported using personal computers. This finding highlights the central role of mobile technology in students' academic, social, and personal activities. The prevalence of smartphone use aligns with global trends in higher education, where mobile devices are increasingly favored for their convenience and accessibility (Partsei et al., 2025). However, this heavy dependence on mobile phones may also heighten vulnerability to cybersecurity risks, as mobile platforms often involve frequent application downloads, unsecured networks, and less stringent security practices (Ikegwu et al., 2025).

In terms of preferred social media platforms, Facebook is the most dominant, with 87.6% of respondents using it. This is followed by TikTok (7.7%) and Instagram (3.4%), while only a very small proportion reported using X (Twitter) and YouTube (0.7% each). Facebook's prominence suggests students are more frequently exposed to cybersecurity threats commonly associated with the platform, such as phishing attacks, privacy breaches, and account compromise (Jain et al., 2021; Osumo et al., 2025). The relatively low use of other platforms suggests that students' cybersecurity experiences and competencies may be largely shaped by their engagement with Facebook rather than by a diverse range of social media environments.

Overall, the findings indicate that the respondents are predominantly from CMC, rely almost exclusively on mobile phones for daily digital activities, and are highly active on Facebook as their primary social media platform. These patterns suggest that initiatives to improve cybersecurity competence should prioritize mobile security practices and platform-specific awareness, with particular attention to Facebook-related risks. Tailoring cybersecurity education to students' actual digital behaviors and platforms may enhance the relevance and effectiveness of such interventions.

Table 3. Level of Competencies in Cybersecurity

Indicators	<i>M</i>	<i>SD</i>	Interpretation
Social Network Safety and Security			
I am selective when joining various social networking sites.	4.17	0.878	High
I limit the messaging options I use on my social networking accounts.	4.07	0.838	High
I limit who can see my online profile and posts to ensure my personal information stays private.	4.24	0.861	Very High
I set login alerts on my social networking platforms for security.	4.38	0.809	Very High
I block spam users and unwanted contacts on social networking sites.	4.39	0.750	Very High
I regularly update my antivirus and security software.	4.22	0.781	Very High
I am cautious when tagging photos with others or my own to protect privacy.	4.33	0.766	Very High
I regularly adjust and apply privacy settings on my social media accounts to control what others can access.	4.34	0.726	Very High
I know how to report illegal or suspicious activities on social media.	4.36	0.683	Very High
Category Mean	4.28	0.788	Very High
Dealing with Fake Information			
I can differentiate between factual information and opinions online.	4.28	0.725	Very High
I verify the information I find on digital platforms before trusting it.	4.34	0.693	Very High
I consult experts or trusted sources to validate information online.	4.19	0.804	High
I use websites to check if the information I see online is true or false.	4.28	0.778	Very High
I am concerned about the credibility and reliability of information I encounter online.	4.36	0.748	Very High
I set aside my personal biases when evaluating information online.	4.24	0.785	Very High
I am aware of how the design and presentation of online content can influence my perception.	4.31	0.705	Very High
I think critically about the context and source of the information I receive online.	4.41	0.682	Very High

Category Mean	4.30 0.740	Very High
Mobile Phone Security Practices		
I lock my mobile phone with a password or PIN.	4.54 0.696	Very High
I regularly back up data stored on my mobile device.	4.40 0.714	Very High
I enable tracking features on my phone in case it gets lost.	4.33 0.755	Very High
I have installed and keep up-to-date security applications on my mobile device.	4.27 0.821	Very High
I frequently update my mobile device's software and security patches.	4.32 0.771	Very High
I avoid installing unwanted or suspicious applications on my phone.	4.37 0.782	Very High
I disconnect from the internet when my mobile device is not in use for security.	4.53 3.022	Very High
I review app reviews and permissions before downloading new applications.	4.38 0.712	Very High
I record my IMEI number to help recover my device if lost.	4.21 0.879	Very High
I reset my phone to factory settings when giving it to others to protect my data.	4.26 0.824	Very High
Category Mean	4.36 0.997	Very High
Managing Digital Footprint		
I regularly review and adjust the privacy settings of my online accounts.	4.36 0.762	Very High
I delete social media accounts or online profiles I no longer use.	4.29 0.785	Very High
I use online tools to monitor and improve my digital footprint.	4.35 0.747	Very High
I avoid sharing personal emotions or sensitive information online.	4.41 0.720	Very High
I review and manage my online activities regularly.	4.39 0.669	Very High
I use a password manager to keep track of my online passwords securely.	4.44 0.690	Very High
I am aware of the audience that views my online activities.	4.44 0.680	Very High
I set personal boundaries and limit my engagement in certain online activities.	4.43 0.689	Very High
Category Mean	4.39 0.718	Very High
Online Privacy and Wi-Fi Safety		
I update and customize privacy settings across all my online platforms.	4.41 0.646	Very High
My messaging apps use end-to-end encryption to protect my conversations.	4.46 0.652	Very High
I am aware of the potential consequences of posting and sharing content online.	4.44 0.670	Very High
I avoid storing private or sensitive information on unsecured or public storage.	4.40 0.700	Very High
I am selective when accepting friend requests or connections online.	4.40 0.690	Very High
I have installed privacy protection software on my devices.	4.37 0.719	Very High
I remove or hide personal information from online platforms that I no longer use.	4.40 0.718	Very High
I am committed to protecting my online privacy seriously.	4.48 0.682	Very High
Category Mean	4.42 0.685	Very High
Application Safety		
I am cautious when downloading new applications, ensuring their reliability.	4.49 0.642	Very High
I read reviews and understand privacy policies before installing apps.	4.39 0.708	Very High
I review and adjust privacy settings of newly installed applications.	4.38 0.697	Very High
I download apps only from trusted and official app stores.	4.41 0.701	Very High
I delete unused or unnecessary apps regularly.	4.45 0.705	Very High
I avoid sharing personal information through applications.	4.48 0.697	Very High
I am aware of apps that track or share my location.	4.37 0.741	Very High
I evaluate the usefulness of an app before installation.	4.44 0.685	Very High
I install security and safety apps to protect my device.	4.42 0.716	Very High
Category Mean	4.42 0.699	Very High
Web Conferencing and Online Meeting Safety		
I update my web conferencing software regularly.	4.32 0.750	Very High
I disable unnecessary features (like screen sharing or recording) during meetings.	4.36 0.745	Very High
I turn off audio and video sharing when not needed.	4.41 0.721	Very High

I explore and configure privacy settings of the web conferencing platform.	4.43 0.674	Very High
I follow the rules and guidelines set by the host during meetings.	4.43 0.689	Very High
I am vigilant about preventing “bombing” or unauthorized access during webinars.	4.40 0.660	Very High
I avoid sharing personal or sensitive information during online meetings.	4.41 0.738	Very High
I access only digital learning resources from trusted sources.	4.43 0.708	Very High
Category Mean	4.40 0.711	Very High
Digital Learning Resources		
I ensure that I access digital learning resources only from trusted and reliable websites.	4.42 0.707	Very High
I pay close attention to the domain or URL of the educational resources before accessing them.	4.47 0.662	Very High
I consult experts to verify the authenticity of educational resources before using them for study.	4.29 0.698	Very High
I consider the language and grammar quality of the educational resources I use.	4.39 0.727	Very High
I check the author’s credentials and affiliations when accessing digital learning materials.	4.39 0.664	Very High
I verify key statements or facts in digital resources by cross-referencing other sources.	4.40 0.685	Very High
I practice good online behavior by thinking carefully before sharing digital learning materials.	4.36 0.757	Very High
I always cite the original source when using ideas from others in my work.	4.41 0.677	Very High
I read and understand user agreements and intellectual property rights before using online content.	4.43 0.674	Very High
I check the Creative Commons license or usage rights of online educational content before use.	4.46 0.711	Very High
Category Mean	4.40 0.696	Very High
Email and Password Safety		
I create strong, complex passwords for my email accounts.	4.44 0.709	Very High
I know how to enable Two-Factor Authentication (2FA) on my email accounts.	4.39 0.740	Very High
I regularly change my email passwords to maintain security.	4.32 0.772	Very High
I use different passwords for different online accounts.	4.30 0.825	Very High
My passwords include a mix of letters, numbers, and special characters.	4.42 0.780	Very High
I am cautious about clicking on suspicious links in emails.	4.46 0.729	Very High
I avoid entering passwords when using public Wi-Fi or in public places.	4.45 0.738	Very High
I always log out of my accounts after finishing my internet activities.	4.49 0.702	Very High
Category Mean	4.41 0.750	Very High
Overall Mean	4.38 0.754	Very High

The results indicate that criminology students in the Second District of North Cotabato reported a very high level of self-reported cybersecurity practices, with an overall mean of 4.38 and a standard deviation of 0.754. This self-report finding suggests that respondents describe themselves as knowledgeable and proactive about protecting their online information; because the measure is entirely self-reported, it should not be read as evidence of objectively demonstrated competency (see Limitations for a discussion of social-desirability bias, acquiescence bias, ceiling effects, and common-method bias as alternative explanations for the uniformly high scores).

Beginning with Social Network Safety and Security, students reported strong practices for managing their online presence. They reported being selective about joining social networking sites (Mean = 4.17, SD = 0.878) and limiting messaging options (Mean = 4.07, SD = 0.838). The highest mean scores were for blocking unwanted contacts (Mean = 4.39, SD = 0.750) and setting login alerts (Mean = 4.38, SD = 0.809). The category mean for social network safety was 4.28 (SD = 0.788), indicating a very high self-reported level of this practice. Participants reported not only recognizing the importance of safeguarding their personal information but also frequently applying measures intended to prevent unauthorized access and mitigate potential online threats (Anudini et al., 2021).

Regarding Dealing with Fake Information, students reported high levels of awareness and critical thinking. They reported being able to differentiate between factual content and opinions (Mean = 4.28, SD = 0.725) and between verified and unverified online information (Mean = 4.34, SD = 0.693).

Consulting experts or trusted sources scored slightly lower (Mean = 4.19, SD = 0.804) but still reflects a high self-reported level. The category mean was 4.30 (SD = 0.740), indicating that students report carefully distinguishing accurate information from false content. This attentiveness is especially relevant in criminology, where reliance on credible sources and accurate data is important for investigations and sound decision-making for future criminology professionals (Karagiannopoulos et al., 2021; Parwani et al., 2022).

In Mobile Phone Security Practices, students consistently reported very high adherence to device protection. Practices such as locking their mobile phones (Mean = 4.54, SD = 0.696), regularly backing up data (Mean = 4.40, SD = 0.714), and disconnecting from the internet when not in use (Mean = 4.53, SD = 3.022 [Author note: this SD is not mathematically plausible for a 1–5 scale with this mean and requires verification against the raw data before submission]) reflect strong self-reported security awareness. The category mean was 4.36 with a standard deviation of 0.997, suggesting that students recognize mobile devices as a key point of vulnerability and report taking corresponding precautions, consistent with their reported use of passwords, regular updates, and a cautious approach to app installation (Mai & Tick, 2021; Frik et al., 2022).

For Managing Digital Footprint, students scored highly in reviewing and adjusting online privacy settings (Mean=4.36, SD=0.762) and using password managers (Mean=4.44, SD=0.690). The category mean of 4.39 and standard deviation of 0.718 suggest that students are aware of the long-term implications of their digital footprint and report taking steps to manage it, consistent with efforts to regulate what they share online and to keep their online identity secure and professional (Saura et al., 2023; Muhammad et al., 2022).

In Online Privacy and Wi-Fi Safety, respondents scored highest on committing to online privacy (Mean = 4.48, SD = 0.682) and enabling end-to-end encryption in messaging apps (Mean = 4.46, SD = 0.652). The category mean was 4.42 (SD = 0.685), indicating a high self-reported level of awareness of secure communication and associated risks, consistent with careful use of privacy settings, encrypted messaging, and selective online interactions (Anudini et al., 2021).

For application safety, students reported being cautious when downloading new applications (Mean = 4.49, SD = 0.642) and when sharing personal information (Mean = 4.48, SD = 0.697). The category mean of 4.42 and standard deviation of 0.699 reflect consistent, cautious self-reported online behavior, indicating that students report both understanding and regularly applying safe application practices to protect their personal data (Zulqadri et al., 2022).

For Web Conferencing and Online Meeting Safety, students reported regularly updating software (Mean = 4.32, SD = 0.750) and configuring platform privacy settings (Mean = 4.43, SD = 0.674). The category mean of 4.40 and a standard deviation of 0.711 suggest that students report being consistently careful about preventing unauthorized access and protecting sensitive information during online meetings, consistent with awareness of risks such as intrusion, data leaks, and accidental exposure of private content in virtual environments (Tewari & Datt, 2021; Jimmy, 2021).

In Digital Learning Resources, students reported verifying content credibility (Mean = 4.29, SD = 0.698) and checking authorship (Mean = 4.39, SD = 0.664). The category mean was 4.40 (SD = 0.696), indicating self-reported responsible digital-learning practices, consistent with verifying sources, assessing content credibility, and following ethical guidelines when using online educational materials (European Union Agency for Cybersecurity, 2022; Lugo et al., 2023).

Lastly, Email and Password Safety showed very high self-reported competency, with creating strong passwords (Mean=4.44, SD=0.709), enabling two-factor authentication (Mean=4.39, SD=0.740), and logging out after internet use (Mean=4.49, SD=0.702). The category mean was 4.41 with an SD of 0.750, indicating that students report managing their email security through strong passwords, protective features, and cautious online behavior, consistent with an awareness of how important secure

communication is for preventing unauthorized access and digital threats (Şenol et al., 2021; Ezugwu et al., 2023).

Overall, the findings show that criminology students report very high levels of self-reported cybersecurity practices across all measured dimensions. These self-reported practices reflect awareness, responsibility, and critical thinking that are relevant to both personal digital safety and professional work in law enforcement or investigative fields; however, because no objective or performance-based measure was administered, these findings should be read as an indicator of students' self-perceived readiness rather than confirmation of demonstrated competency.

Table 4. Kruskal-Wallis Test of Cybersecurity Competency by School

School	n	M	SD
CMC	165	4.40	0.43
MIST	83	4.37	0.46
CDK	50	4.32	0.35
H(2)			2.885
p-value			.236

In Table 4, the Kruskal–Wallis test examined potential differences in cybersecurity competency among criminology students from Central Mindanao Colleges (CMC), MIST, and CDK. Students from CMC recorded the highest mean score ($M = 4.40$, $SD = 0.43$), followed closely by MIST ($M = 4.37$, $SD = 0.46$) and CDK ($M = 4.32$, $SD = 0.35$). The Kruskal–Wallis statistic was $H(2) = 2.885$, $p = 0.236$, which exceeds the 0.05 threshold. This indicates no statistically significant difference among the schools.

It is important to clarify that the absence of statistical significance does not confirm equality or uniformity in competency; rather, it suggests that any observed differences were not detectable with the current sample. Therefore, conclusions such as “institutional affiliation does not influence competency” should be interpreted cautiously. A more precise framing is that students across these institutions demonstrate comparable cybersecurity competency within the scope of this study.

From a theoretical perspective, PMT (Rogers, 1975; Floyd et al., 2000) offers one possible interpretive lens for this outcome: students may perceive cyber threats similarly across institutions, which could encourage comparable protective cybersecurity behaviors regardless of school; this interpretation is offered cautiously, as perceived threat and coping appraisal were not directly measured. Similarly, TAM (Davis, 1989; Dash & Ansari, 2022) suggests that individuals adopt digital practices, including cybersecurity behaviors, when they perceive technologies as useful and user-friendly, although this study did not directly measure perceived usefulness and ease of use. The study did not assess whether schools provided comparable exposure to digital learning environments, and this should not be assumed. Although some literature suggests that differences in institutional resources may influence cybersecurity competency (Ibrahim et al., 2024), the participating institutions in the current study may have relatively similar digital infrastructures, which could explain the non-significant differences observed.

Table 5. Kruskal-Wallis Test of Cybersecurity Competency by Primary Device Used

Device	n	M	SD
Mobile Phone	291	4.38	0.43
Laptop	3	4.23	0.27
Personal Computer	3	3.94	0.52
H(2)			3.677
p-value			.159

Table 5 shows that students who primarily used mobile phones achieved the highest mean competency ($M = 4.38$, $SD = 0.43$), followed by laptop users ($M = 4.23$, $SD = 0.27$) and personal

computer users ($M = 3.94$, $SD = 0.52$). The Kruskal–Wallis test yielded $H(2) = 3.677$ and $p = 0.159$, indicating no statistically significant differences across device types. These findings indicate no statistically detectable difference in self-reported cybersecurity competency between device types in this sample. Although mobile phone users scored slightly higher, the differences were small, not statistically significant, and should not be interpreted as evidence that device type has no effect, particularly given the extremely unequal group sizes described below.

The extremely unequal group sizes ($n = 291$ for mobile, $n = 3$ for laptops, $n = 3$ for personal computers) substantially limited statistical power and the stability of the subgroup estimates. Consequently, the nonsignificant result should not be interpreted as evidence that cybersecurity competency is equivalent across device types; PMT-based explanations, such as students encountering comparable cyber threats (e.g., phishing or malware) regardless of device, remain a plausible but untested interpretation, consistent with prior findings that digital experience, rather than the specific device used, is associated with cybersecurity awareness (Althibyani & Al-Zahrani, 2023; Sarfi et al., 2023).

Table 6. Kruskal–Wallis Test of Cybersecurity Competency by Preferred Social Media

Social Media Site	n	M	SD
Facebook	261	4.38	0.43
TikTok	23	4.47	0.42
Instagram	10	4.09	0.36
X (Twitter)	2	4.53	0.46
YouTube	2	4.27	0.34
H(4)			6.900
p-value			.141

Table 6 indicates slight variations in cybersecurity competency across social media platforms, with X (Twitter) users scoring highest ($M = 4.53$, $SD = 0.46$) and Instagram users lowest ($M = 4.09$, $SD = 0.36$). The Kruskal–Wallis test yielded $H(4) = 6.900$ and $p = 0.141$, suggesting no statistically significant differences among groups. This result indicates no statistically detectable difference in self-reported cybersecurity competency across preferred social media platforms in this sample. Minor variations in mean scores are insufficient to conclude that any one platform is associated with greater cybersecurity awareness, particularly given the small size of most platform subgroups (see below). From the TAM perspective, most platforms offer broadly similar security features (e.g., privacy settings, account verification, multi-factor authentication), which may be one reason users report comparable cybersecurity behaviors; PMT similarly offers a plausible, though untested, explanation that exposure to online risks across platforms motivates protective behavior independent of platform preference.

The large disparity in sample sizes (261 Facebook users versus 2–23 users across other platforms) substantially limits the statistical power of this comparison, and the near-absence of respondents in several platform categories means these subgroup results should be treated as descriptive rather than conclusive. With that caveat, the consistently high self-reported competency scores are broadly consistent with prior research suggesting that digital literacy and general online experience, rather than platform-specific features, shape self-reported cybersecurity behavior (Karagiannopoulos et al., 2021; Umejiaku & Uzoka, 2022).

Across all analyses, nonsignificant results consistently indicate that differences were not statistically detectable in this sample, not that the compared groups are truly equivalent — a distinction that is especially important given the very small and highly unequal subgroup sizes for device and social-media comparisons. Within these limits, the findings suggest that criminology students in the Second District of North Cotabato report broadly similar levels of self-reported cybersecurity competency across school, device, and platform groups. PMT and TAM are used here as interpretive frameworks for discussing these patterns rather than as directly tested models: students' perceptions of cyber threats, motivation to protect themselves, and interactions with user-friendly digital tools are

plausible contributors to the generalized protective behaviors reported across schools, devices, and social media platforms, though none of these constructs were directly measured. If future research corroborates these constructs, this pattern suggests that interventions to strengthen cybersecurity awareness may be most effective when implemented at the programmatic or district level, targeting general digital behaviors and risk management rather than institution-specific or device-specific approaches.

4. Conclusion

Among incoming fourth-year criminology students with prior cybersecurity exposure, respondents reported high engagement in cybersecurity and digital-safety practices across all instrument dimensions. They self-identify as aware of common cyber threats, report regularly practicing precautionary measures, and report engaging responsibly in digital environments. Because the data are based solely on self-reported measures, with no objective assessment of knowledge, skills, or observed behavior, these findings should not be interpreted as evidence of objectively demonstrated cybersecurity competency. In terms of inferential analysis, the study found no statistically significant differences in students' self-reported cybersecurity competency by school, primary device used, or preferred social media platform. The study did not conduct mediation or moderation analyses and made no claims about mediating or moderating effects. Given the highly unequal and, for device and platform, very small subgroup sizes, these nonsignificant results should be interpreted as an absence of statistically detectable differences in this sample, not as evidence that competency is equivalent or stable across these factors; conclusions regarding device and social-media platform comparisons in particular should be treated with caution given the small size of most subgroups.

Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM) were used as interpretive lenses for discussing the findings rather than as directly tested frameworks: their core constructs (e.g., perceived severity, self-efficacy, perceived usefulness, perceived ease of use) were not measured in this study. The findings are therefore broadly consistent with, but do not directly test or confirm, either theory. In conclusion, while students in this study perceive themselves as knowledgeable and proactive in cybersecurity practices, these conclusions are limited to a selected sample of students with prior cybersecurity exposure and to self-reported data. Future research should (1) conduct practical cybersecurity simulations or knowledge tests to objectively verify students' skills and behaviors; (2) embed phishing identification, password security, evidence preservation, mobile-device security, and digital-forensics exercises in criminology courses; (3) use pretest–posttest designs to evaluate the effectiveness of such training; (4) compare self-perceived competency with objectively tested performance; and (5) examine curriculum exposure itself as an explanatory variable. District-wide policy recommendations should not be based solely on descriptive self-report data from three purposively selected institutions.

5. Limitations of the Study

This study has several limitations that should inform the interpretation of its findings. First, the cross-sectional descriptive-comparative design cannot establish change over time or causal relationships. Second, the study relied exclusively on self-report, which is subject to social-desirability and recall biases and does not capture objectively demonstrated skill; the uniformly high, positively worded item scores are also consistent with ceiling effects and common-method bias, in addition to genuinely high self-perceived competency. Third, the inclusion criterion requiring prior cybersecurity exposure introduces selection bias and likely inflates competency estimates relative to the full incoming fourth-year population; findings apply only to students with prior exposure. Fourth, the adapted Cybersecurity Competency Scale was originally developed for prospective teachers, and its content and construct validity for criminology students, including its factor structure, has not been independently confirmed in the present sample. Fifth, sampling combined proportionate stratification by school with convenience selection within each stratum, is limited to three purposively selected institutions within one district, and may have involved nonprobability selection within strata; these features restrict

generalizability beyond the studied institutions and district. Sixth, comparisons by primary device and by preferred social media platform involved extremely unequal and, for several categories, very small groups (as few as two or three respondents), which substantially limited statistical power and the stability of those estimates; these comparisons should be treated as descriptive rather than conclusive. Finally, several potentially relevant variables were not controlled or measured, including formal coursework content and duration, training duration, home internet access, prior cyber-victimization, socioeconomic status, and general digital experience; future studies should measure these variables and complement self-report with objective or performance-based assessment.

Supplementary Details

Supplementary Materials & Data availability statement (If Applicable):

The data that support the findings of this study are available from the corresponding author upon reasonable request. The data are not publicly available due to privacy and confidentiality restrictions, as they contain information that could compromise the anonymity of the research participants.

Author Contributions:

All authors were responsible for the conceptualization and design of the study, development and validation of the research instrument, data collection and analysis, interpretation of findings, and preparation and revision of the manuscript. The authors also reviewed and approved the final version of the manuscript and accepted responsibility for the integrity and accuracy of the work.

Funding:

This research received no external funding.

Institutional Review Board Statement

Not applicable. The study was conducted in accordance with ethical standards for educational research. Necessary permissions were secured from the concerned educational authorities and participating schools prior to the conduct of the study.

Informed Consent Statement:

The study adhered to ethical standards in research involving human participants. Prior to data collection, participants were provided with a comprehensive informed consent form detailing the purpose of the study, procedures, potential risks and benefits, confidentiality measures, and their rights, including voluntary participation and the option to withdraw at any time without

Acknowledgments:

The authors sincerely thank all the respondents who participated in this study and generously shared their time, experiences, and insights. Their participation made the completion of this research possible.

Conflicts of Interest:

The authors declare no conflict of interest.

Disclosure Statement:

The authors used Grammarly only for language editing. No AI tools were used in the data analysis or in generating the study's results. The authors reviewed and validated all content and took full responsibility for the article's accuracy, originality, and integrity.

References

- Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, 5(2), 23. <https://doi.org/10.3390/bdcc5020023>
- Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. *Sustainability*, 15(15), 11512. <https://doi.org/10.3390/su151511512>

- Anudini, A. K. S. A., Dissanayake, H. M. S. S., & Uwanthika, G. A. I. (2021). Impact of social media-related cybercrimes and preventive precautions. *In 14th International Research Conference* (p. 460).
- Bendler, D., & Felderer, M. (2023). Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model. *ACM Transactions on Computing Education*, 23(2), 1–33.
- Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, 28(2), 1809–1831.
- Cleland, J., Alexander, K., & Poobalan, A. (2023). Sampling and recruiting participants. *In Starting Research in Clinical Education* (pp. 47–56). Wiley Blackwell.
- CNNIC. (2022). The 49th statistical report on internet development in China. China Internet Network Information Center. <http://www.cnnic.net.cn/hlwfzyj/hlwzxbg/>
- Dapitan, J. U., Butchayo, J. M. M., Palma, J. L. R., Arevalo, M. A., Alvarico, A. B., & Cuevas, J. F., Jr. (2024). Measuring the level of cybersecurity awareness among senior high school students. *Mediterranean Journal of Basic and Applied Sciences*, 8(2), 208–217.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- European Union Agency for Cybersecurity. (2022). European Cybersecurity Skills Framework. ENISA. <https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework>
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407–429.
- Frik, A., Kim, J. L., Sanchez, J. R., & Ma, J. (2022). Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3491102.3517504>
- Hazarika, H. J. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. Alexandria: *The Journal of National and International Library and Information Issues*. Advance online publication. <https://doi.org/10.1177/09557490251340833>
- Ibrahim, A., McKee, M., Sikos, L., & Johnson, N. (2024). A systematic review of K-12 cybersecurity education around the world. *IEEE Access*, 12, 59726–59738. <https://doi.org/10.1109/ACCESS.2024.3393425>
- Ikegwu, A. C., Alo, U. R., & Nweke, H. F. (2025). Cyber threats in mobile healthcare applications: Systematic review of enabling technologies, threat models, detection approaches, and future directions. *Discover Computing*, 28(1), 152.
- Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex & Intelligent Systems*, 7, 2157–2177. <https://doi.org/10.1007/s40747-021-00409-7>
- Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, 1, 564–574.
- Karagiannopoulos, V., Kirby, A., Ms, S. O. M., & Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, 43, 105615.
- Lugo, R. G., Sütterlin, S., Knox, B. J., Bukauskas, L., Brilingaitė, A., & Maennel, O. M. (2023). The human factor in cyber security education. *Frontiers in Education*, 8, 1277282.
- Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, 18(8). <https://doi.org/10.12700/aph.18.8.2021.8.4>

- Morgan, S. (2020). Cybercrime to cost the world \$10.5 trillion annually by 2025. Cybersecurity Ventures. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- Muhammad, S. S., Dey, B. L., Syed Alwi, S. F., Kamal, M. M., & Asaad, Y. (2022). Consumers' willingness to share digital footprints on social media: The role of affective trust. *Information Technology & People*. Advance online publication. <https://doi.org/10.1108/itp-10-2020-0694>
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.
- Osumo, L. G., Aguilar, A., Ceniza, A. L., & Javines, J. (2025). Hashtags and politics: A mixed-methods study on Generation Z's influence of social media on political participation in Makilala, Cotabato. *Asia Pacific Journal of Educational Technologies, Psychology, and Social Sciences*, 1(2). <https://doi.org/10.70847/660413>
- Partsei, K., Shevchuk, B., Buksar, S., Kurtyak, F., & Barabanchyk, O. (2025). The impact of using mobile apps on student engagement and involvement in the learning process. *Periodicals of Engineering and Natural Sciences*, 13(1), 219–232.
- Parwani, P., Nikose, P., & Rathor, J. (2022). Awareness regarding cyber crime among people. *International Journal of Research Publication and Reviews*, 3(1), 944–947.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Santhosh, T., & Thiyagu, K. (2024). Development and validation of cyber security competency scale for prospective teachers. *Journal of Pedagogical Sociology and Psychology*, 6(3), 111–124.
- Sarfi, M., Darvishii, M., & Zohouri, M. (2023). Why people may view online crimes as less criminal: Exploring the perception of cybercrime. *International e-Journal of Criminal Sciences*, 18.
- Saura, J. R., Palacios-Marqués, D., & Ribeiro-Soriano, D. (2023). Privacy concerns in social media UGC communities: Understanding user behavior sentiments in complex networks. *Information Systems and e-Business Management*. Advance online publication. <https://doi.org/10.1007/s10257-023-00631-5>
- Tewari, N., & Datt, G. (2021). A study on the systematic review of security vulnerabilities of popular web browsers. In *2021 International Conference on Technological Advancements and Innovations (ICTAI)* (pp. 314–318). IEEE.
- Umejiaku, N., & Uzoka, N. (2022). An overview of social media related cybercrimes and its legal remedy. *Law View*.
- Zulqadri, D. M., Mustadi, A., & Retnawati, H. (2022). Digital safety during online learning: What we do to protect our student? *Jurnal Iqra': Kajian Ilmu Pendidikan*, 7(1), 178–191.