PANTAO
The International Journal of the Humanities and Social Sciences
Volume 5, Issue 1
ISSN 3028-0877 | DOI 10.69651/2022PIJHSS

The effects of exposure to online activities on cybersecurity awareness among rural internet users

Jodi V. Garcia*
Biabas Trade High School
Bohol, Philippines

Jane C. Adlawon
Biabas Trade High School
Bohol, Philippines

Ethel V. Cutamora
Biabas Trade High School
Bohol, Philippines

Mary Grace S. Vallente
Biabas Trade High School
Bohol, Philippines

Katrina M. Sarol
Biabas Trade High School
Bohol, Philippines

Rhea B. Aumentado
Biabas Trade High School
Bohol, Philippines

Christlyn Mary B. Versales
Biabas Trade High School
Bohol, Philippines

Lyka A. Sanchez
Biabas Trade High School
Bohol, Philippines

Zaldy H. Bacus
Biabas Trade High School
Bohol, Philippines
Email: zaldybacus30@gmail.com

*Corresponding author
DOI: http://doi.org/10.69651/PIJHSS0501845

Recommended citation:
Garcia, J. V., Sarol, K. M., Adlawon, J. C., Aumentado, R. B., Cutamora, E. V., Versales, C. M. B., Vallente, M. G. S., Sanchez, L. A., & Bacus, Z. H. (2026). The effects of exposure to online activities on cybersecurity awareness among rural internet users. Pantao (The International Journal of the Humanities and Social Sciences) 5 (1), 9535-9545. http://doi.org/10.69651/PIJHSS0501845

ABSTRACT

This study investigated the effects of online activity exposure on the cybersecurity awareness of 70 randomly selected internet users in Barangay Biabas, Ubay, Bohol, during the 2025–2026 period. Employing a descriptive correlational research design, the researchers utilized a validated researcher-made questionnaire to gather data across seven puroks to ensure balanced community representation. The process involved securing official permissions, conducting on-site surveys, and analyzing data through One-Way ANOVA and Pearson Product Moment Correlation to determine significant differences and relationships. Results revealed that while respondents predominantly aged 15 to 20 and frequent Facebook users possess a very high perception of online exposure and safety, they struggle with technical understanding and proactive threat preparedness. Statistical testing confirmed a significant positive relationship ($r = 0.927417$) between digital engagement and cybersecurity knowledge, implying that increased time spent online naturally fosters basic safety skills. However, the findings also highlight a critical gap in verifying information legitimacy and compliance with the Cybercrime Prevention Act of 2012. The study concludes that while regular internet use builds foundational awareness, it is insufficient for navigating evolving technical threats or official legal standards. Consequently, it is recommended that the Barangay Local Government Unit and the Department of Telecommunication collaborate to implement the "Safe Digital Biabas" program. This action plan focuses on monthly seminars and localized Facebook-based safety campaigns to bridge the gap between basic practice and technical proficiency for all residents.

Keywords: Cybersecurity awareness, online activity exposure, digital engagement, descriptive correlative design, proactive threat preparedness, technical proficiency, Safe Digital Biabas Program, internet user behavior

Date Submitted: January 27, 2026
Date Accepted: February 5, 2026
Date Published: February 25, 2026

INTRODUCTION

The internet is a global network that enables people to communicate, access information, and share resources. Vogels et al. (2022) stated that more than half of the world's population were active internet users. They also noted that social media, online shopping, remote work applications, and on-demand entertainment have significantly reshaped everyday life. Exposure to online activities referred to the time, frequency, and type of engagement on platforms like social media and websites, while cybersecurity awareness referred to understanding online threats and safe digital practices. In Barangay Biabas, residents used online platforms for communication, education, and daily routines, which gave them opportunities to learn but also exposed them to risks. Many residents lacked sufficient knowledge of safe online practices, putting them at risk of scams, phishing, and identity theft. This study will examine how exposure to online activities affect cybersecurity awareness.

Exposure to online activities helps users access information, communication tools, and online services that support their daily needs. Cybersecurity awareness protects users from online scams, identity theft, and harmful digital attacks. Together, these variables influence how safe and responsible internet users can be in a community. Previous studies have explored online exposure and cybersecurity awareness, but most focused on larger populations or urban areas, leaving small communities like Barangay Biabas understudied. More online exposure can help people learn new digital skills, but it can also increase their vulnerability to cyber risks

if they are not properly informed. High engagement in social media may improve connection with others, yet it also opens doors to fake news, phishing links, and suspicious accounts. Online shopping offers convenience, but users may face fraud if they lack cybersecurity knowledge. Educational content online can teach residents helpful skills, but unreliable websites may expose them to malware. Online entertainment allows relaxation, but it can also expose users to unsafe content. Exposure to online activities affects cybersecurity awareness by determining how often residents encounter online risks and how well they can respond to them. This study was chosen to understand how exposure to online activities influences residents' cybersecurity awareness and to explore ways to improve safe internet practices in Barangay Biabas.

This study aims to identify how residents' exposure to online activities influences their level of cybersecurity awareness. It also seeks to understand the risks residents commonly face online and how their awareness affects their digital safety. Ultimately, the study strives to recommend strategies that will strengthen the cybersecurity knowledge and safe online practices of internet users in Barangay Biabas.

Statement of the problem

This study aims to investigate the effects of residents' exposure to online activities on the cybersecurity awareness of internet users in Barangay Biabas during the year 2025 2026. Specifically, it seeks to determine how demographic characteristics, exposure to online activities, and levels of cybersecurity awareness relate to one another and to identify possible recommendations based on the findings.

1. What is the demographic profile of the respondents in terms of age, sex, average daily hours spent online, frequency of internet use, and online platforms used?
2. What is the perception of the respondents regarding their exposure to online activities in terms of awareness to online threats, legitimacy of information, and consequences of online activities on daily lives?
3. What is the level of cybersecurity awareness among the internet users in Barangay Biabas in terms of knowledge of cybersecurity awareness, understanding of cybersecurity concepts, and application of safe online practices to protect online activities?
4. Is there a significant difference in the perception of the respondents regarding their exposure to online activities across the different demographic profiles of the respondents?
5. Is there a significant difference in the level of cybersecurity awareness across the different demographic profiles of the respondents?
6. Is there a significant relationship between the perception of the respondents regarding their exposure to online activities and their level of cybersecurity awareness?
7. Based on the study, what recommendations can be made?

METHODOLOGY

This study employs a descriptive correlational method to examine the effect of exposure to online activities on the cybersecurity awareness of internet users in Barangay Biabas. This approach allows the researchers to describe the current online behaviors of respondents while determining whether a significant relationship exists between the frequency and type of online exposure and their level of cybersecurity awareness. Through this method, the study identifies

patterns, compares responses, and statistically analyzes how different online activities influence residents' understanding and practice of safe internet usage.

The research is conducted in Barangay Biabas, which serves as the actual setting where internet use and online activities occur among residents. This locale provides direct access to internet users who are exposed to various online platforms. It allows the researchers to observe and assess the level of cybersecurity awareness of respondents during the year 2025 2026.

The respondents of this study are selected through simple random sampling, focusing specifically on residents who actively use the internet in their daily activities. A total of 70 respondents are included, representing regular internet users within their respective communities. To ensure balanced representation, respondents are chosen from different age, sex, and online usage backgrounds. These individuals are selected because of their direct experience with online platforms such as social media, communication applications, and online services. The inclusion criteria cover residents of Barangay Biabas who use the internet daily and are willing to participate in the study, while those with limited or no internet access, or those unwilling to complete the survey, are excluded.

The study utilizes a researcher made questionnaire as the primary tool for data gathering. The questionnaire is designed to determine how often residents go online and how aware they are of online risks. It is administered through a simple survey and includes questions about the respondents' background, online activities, and knowledge of cyber safety. The researchers review the questionnaire to ensure that the questions are clear and easy to understand, thereby enabling respondents to provide accurate and useful answers for the study.

A systematic data gathering procedure is followed to ensure the accuracy and reliability of the information collected. The researchers first secure permission by writing a formal request addressed to the barangay officials of Barangay Biabas. The letter includes the research title, purpose, target respondents, and requested dates for data collection. Upon approval, coordination with barangay leaders is conducted to identify available internet users in the community, and informed consent forms are prepared and secured from all participants prior to survey administration. The researchers then prepare a structured researcher made survey questionnaire based on the statement of the problem concerning the effects of exposure to online activities on cybersecurity awareness. The instrument includes sections on the respondents' demographic profile, exposure to online activities, and level of cybersecurity awareness, and it is reviewed by a teacher to ensure clarity, relevance, and content validity.

Following approval and preparation, the survey is administered to identified internet users in Barangay Biabas. The purpose of the study is explained to the participants, and they are assured of confidentiality and voluntary participation. The questionnaires are distributed individually, and respondents complete them in a comfortable and quiet area. The researchers remain available to clarify instructions without influencing any responses, and sufficient time is provided for participants to complete the survey. Upon completion, the accomplished questionnaires are immediately retrieved to prevent loss, damage, or misplacement. Each form is checked for completeness and readability, and respondents are politely asked to supply any missing answers while still present. The retrieved questionnaires are then coded and organized according to respondent categories to ensure proper sorting and recording. All data are stored securely in properly labeled folders or envelopes to prevent loss during the process.

The collected responses undergo data analysis, wherein the information is organized, tallied, and interpreted in accordance with the objectives of the study. This process ensures that the gathered data are systematically examined to determine patterns, relationships, and levels of cybersecurity awareness among the respondents.

Ethical considerations are strictly observed throughout the study. The research undergoes an ethics review by the Research Committee of Biabas Trade High School. After

securing the necessary permissions from the administration, the researchers explain the purpose of the study to the respondents. Participation is entirely voluntary, and respondents are not subjected to any form of harm. They are informed of their right to withdraw from the study at any stage without consequence. The dignity of the respondents is upheld, and their privacy is protected at all stages of the research. Adequate levels of confidentiality are maintained to safeguard all collected data. Participation is based on informed consent, wherein respondents are provided with sufficient information and assurances to fully understand the implications of their involvement and to make a free and informed decision without any pressure or coercion. The researchers adhere to the No Harm Policy, and anonymity is prioritized in conducting the study. A debriefing session with the barangay captain is conducted in the event of any adverse effect related to the study.

RESULTS AND DISCUSSION

This section presents the results and discussion of the study based on data gathered from 70 respondents using a descriptive correlational research design and simple random sampling technique. The data were collected through a researcher made questionnaire and analyzed using descriptive statistics, weighted means, One Way ANOVA, and Pearson Product Moment Correlation. The discussion is grounded on the data obtained and is interpreted in direct relation to the objectives of the study, focusing on the respondents' demographic profile, their perception of exposure to online activities, their level of cybersecurity awareness, and the relationships and differences among the identified variables.

The demographic profile of the respondents reveals that out of 70 participants, 33 or 47.14% are aged 15 to 20 years old, 10 or 14.29% are aged 21 to 25 years old, and 27 or 38.57% are aged 26 to 30 years old above. In terms of sex, there is an equal distribution with 35 or 50% male and 35 or 50% female respondents. Regarding average daily hours spent online, 6 or 8.57% spend 1 hour, 8 or 11.43% spend 2 hours, and a majority of 56 or 80% spend more than 3 hours online. In terms of frequency of internet use, 65 or 92.86% use the internet daily, 3 or 4.29% weekly, and 2 or 2.86% monthly. With respect to online platforms used, Facebook is the most utilized platform with 43 or 61.43%, followed by Loklok with 10 or 14.29%, TikTok with 8 or 11.43%, Messenger with 6 or 8.57%, and Instagram with 3 or 4.29%, while Twitter, YouTube, WhatsApp, and Google Classroom recorded 0 or 0%. These findings suggest that the respondents are predominantly young, highly active internet users who engage frequently with social media platforms, particularly Facebook, which aligns with Bandura's Social Cognitive Theory that emphasizes observational learning through digital environments.

The perception of respondents regarding their exposure to online activities indicates a very high level across all indicators. In terms of awareness of online threats, the composite mean is 3.79, interpreted as Strongly Agree within the scale of 3.51 to 4.00. Individual item means range from 3.73 to 3.84, with the highest values of 3.84 for recognizing the need to watch how others face online threats and being conscious of online risk, both ranked 1.5, and the lowest value of 3.73 for knowing about new online threats, ranked 10. These results indicate that while respondents are highly aware of online threats, they are less consistent in updating their knowledge about emerging risks, reflecting experiential learning as explained by Bandura's Social Cognitive Theory. In terms of legitimacy of information, the composite mean is 3.78, also interpreted as Strongly Agree. The highest weighted means of 3.83 are observed for choosing reliable sources and evaluating online content, both ranked 1.5, while the lowest mean of 3.70 corresponds to questioning inconsistent information, ranked 10. This suggests that respondents rely on familiar and trusted sources but may not engage in deeper verification processes, which is consistent with the Unified Theory of Acceptance and Use of Technology

that highlights users' tendency to avoid effort intensive tasks. Regarding the consequences of online activities on daily lives, the composite mean is 3.78, interpreted as Strongly Agree. The highest mean of 3.83, ranked 1, reflects planning online activities to prevent negative effects, while the lowest mean of 3.71, ranked 10, relates to considering how online activities affect daily life. This indicates that respondents prioritize immediate control of online behavior over long term reflection, which aligns with Ajzen's Theory of Planned Behavior emphasizing action based on perceived immediate benefits. Overall, the weighted mean for perception is 3.78, interpreted as Strongly Agree, with awareness of online threats ranked first at 3.79, and both legitimacy of information and consequences of online activities ranked 2.5 at 3.78, demonstrating a consistently high perception across dimensions.

The level of cybersecurity awareness among respondents is also very high across all indicators. For knowledge of cybersecurity awareness, the composite mean is 3.81, interpreted as Strongly Agree, with individual means ranging from 3.76 to 3.83. The highest means of 3.83, ranked 2, reflect awareness of online threats, knowledge of cybersecurity, and adherence to cybersecurity rules, while the lowest mean of 3.76, ranked 10, corresponds to understanding how cybersecurity works. This indicates strong awareness of rules but limited understanding of technical mechanisms, consistent with Rogers' Protection Motivation Theory. For understanding of cybersecurity concepts, the composite mean is 3.81, interpreted as Strongly Agree, with the highest mean of 3.86, ranked 1, for organizing cybersecurity information, and the lowest mean of 3.74, ranked 10, for building knowledge about cybersecurity concepts. This suggests that respondents are more adept at organizing existing knowledge than exploring new concepts, consistent with the Social Identity Model of Deindividuation Effects Theory. In terms of application of safe online practices, the composite mean is 3.83, interpreted as Strongly Agree, with the highest means of 3.86, ranked 1.5, for taking precautions and controlling online activities, and the lowest means of 3.79, ranked 9.5, for using safe practices and obeying rules. This indicates that respondents practice safety behaviors but may not consistently adhere to formal guidelines such as the Cybercrime Prevention Act of 2012. The overall weighted mean for cybersecurity awareness is 3.82, interpreted as Strongly Agree, with application ranked first at 3.83, followed by knowledge and understanding both at 3.81, highlighting a stronger emphasis on practice than conceptual understanding.

The analysis of differences in perception of exposure to online activities across demographic profiles using One Way ANOVA shows that age has a computed value of 1.760297 compared to a tabular value of 3.133762, indicating Not Significant and leading to acceptance of the null hypothesis. Sex has a computed value of 0.998633 compared to 3.981896, also Not Significant, resulting in acceptance of the null hypothesis. Daily hours spent online has a computed value of 20.64621 compared to 3.133762, which is Significant, leading to rejection of the null hypothesis. Frequency of internet use has a computed value of 6.081706 compared to 3.133762, also Significant, resulting in rejection of the null hypothesis. Online platforms used has a computed value of 0.793105 compared to 2.094286, indicating Not Significant and acceptance of the null hypothesis. These results demonstrate that perception of online exposure is significantly influenced by the amount of time and frequency of internet use, while age, sex, and platform type do not significantly affect perception, supporting Bandura's Social Cognitive Theory that emphasizes environmental exposure as a key factor in learning.

Similarly, the analysis of differences in the level of cybersecurity awareness across demographic profiles shows that age has a computed value of 3.35364 compared to 3.133762, indicating Significant and leading to rejection of the null hypothesis. Sex has a computed value of 0.518275 compared to 3.981896, indicating Not Significant and acceptance of the null hypothesis. Daily hours spent online has a computed value of 19.13359 compared to 3.133762, which is Significant, resulting in rejection of the null hypothesis. Frequency of internet use has

a computed value of 6.045534 compared to 3.133762, also Significant, leading to rejection of the null hypothesis. Online platforms used has a computed value of 0.739057 compared to 2.094286, indicating Not Significant and acceptance of the null hypothesis. These findings indicate that cybersecurity awareness is significantly influenced by age, daily hours spent online, and frequency of use, while sex and platform choice do not have significant effects. This aligns with the Unified Theory of Acceptance and Use of Technology, which emphasizes the role of facilitating conditions and usage behavior in shaping technology related competencies.

The relationship between perception of exposure to online activities and level of cybersecurity awareness is examined using Pearson Product Moment Correlation, yielding a computed r value of 0.927417, which indicates a very high positive correlation. The computed t value of 20.44672 exceeds the tabular t value of 1.995, confirming that the relationship is statistically Significant and leading to rejection of the null hypothesis. This result demonstrates that increased exposure to online activities is strongly associated with higher levels of cybersecurity awareness. The findings suggest that frequent and sustained engagement with digital environments enhances users' ability to recognize threats, adopt protective behaviors, and develop cybersecurity competencies. This supports the view that experiential learning and repeated exposure play critical roles in developing digital literacy, while also highlighting the need for structured interventions to guide users toward compliance with formal cybersecurity standards.

In synthesis, the findings reveal that the respondents are highly active internet users with very high levels of perception and cybersecurity awareness, particularly in practical application. The results confirm that exposure to online activities significantly influences cybersecurity awareness, as evidenced by the strong positive correlation of r = 0.927417 and significant differences based on daily hours spent online and frequency of use. While respondents demonstrate strong awareness and safe practices, gaps remain in deeper conceptual understanding and critical evaluation of information. These findings contribute to the understanding of cybersecurity behavior among rural internet users by emphasizing the importance of digital exposure and experiential learning, while also underscoring the need for targeted educational interventions. The results provide a clear basis for developing recommendations aimed at enhancing cybersecurity awareness and will guide the subsequent section of the study.

CONCLUSION

The study concludes that the investigation successfully established the key connections between exposure to online activities and cybersecurity awareness among internet users aged 15 and above in Barangay Biabas, Ubay, Bohol. The findings revealed that most respondents belong to the 15 to 20 age group, engage in daily internet use, and primarily utilize Facebook as their main platform, indicating a very high level of online engagement within the community. Statistical results confirmed that the amount of time spent online and the frequency of internet use significantly influence both the perception of online exposure and the level of cybersecurity awareness, whereas sex and the type of online platform used do not have a significant effect. Furthermore, the study demonstrated a very strong and significant relationship between exposure to online activities and cybersecurity awareness, confirming that increased digital engagement is directly associated with higher levels of awareness and safer online practices.

Despite the very high levels of perception and cybersecurity awareness observed among respondents, the findings also revealed important gaps that require attention. While users are

generally knowledgeable about basic cybersecurity practices and demonstrate caution in their online activities, they do not consistently keep up with emerging online threats, critically verify the legitimacy of information, fully understand how cybersecurity tools function, or strictly adhere to established regulations such as the Cybercrime Prevention Act of 2012. These results indicate that although regular internet use contributes to the development of practical online safety skills, it is not sufficient to ensure comprehensive cybersecurity competence. There remains a need for structured, continuous, and guided learning to strengthen deeper understanding, critical evaluation skills, and compliance with formal cybersecurity standards.

In light of these findings, the study underscores the importance of targeted and collaborative interventions to address the identified gaps. Internet users are encouraged to actively update their knowledge of emerging online threats by following credible sources such as official government pages and local announcements, to practice consistent verification of online information before accepting or sharing it, and to develop a deeper understanding of cybersecurity tools including antivirus software and two factor authentication. At the community level, the Barangay Local Government Unit is encouraged to organize regular cybersecurity seminars, particularly on a monthly basis, focusing on emerging threats, fact checking techniques, and adherence to national cybersecurity policies. The development of community based digital safety programs, with sessions conducted in each purok and in partnership with local schools, is also essential to strengthen awareness among different age groups.

At the institutional level, the Department of Telecommunication is encouraged to assess existing cybersecurity initiatives within Barangay Biabas to identify areas that require improvement and enhancement. The development of simple and accessible instructional materials explaining the functions of cybersecurity tools, the updating of local guidelines to address evolving digital risks, and the strengthening of communication strategies to ensure adherence to official standards such as the Cybercrime Prevention Act are recommended. In addition, researchers are encouraged to further explore how specific online platforms such as Facebook influence cybersecurity awareness differently and to investigate more effective approaches to digital safety education across various demographic groups.

Moreover, future researchers are encouraged to extend this study by designing and testing structured cybersecurity training programs to evaluate their effectiveness in addressing the identified knowledge gaps. Follow up studies are also recommended to examine the underlying reasons for persistent gaps in cybersecurity awareness and to explore how community based initiatives can be expanded and replicated in other areas of Ubay, Bohol. Further investigations may also focus on developing targeted and context specific interventions for different segments of the population to ensure inclusive and sustainable cybersecurity education.

Overall, the study affirms that while exposure to online activities plays a critical role in enhancing cybersecurity awareness, it must be complemented by systematic education, community engagement, and institutional support to ensure that internet users are not only active but also informed, critical, and responsible participants in the digital environment.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of cybercrime and legal awareness on the behavior of University of Jordan students. Heliyon. https://doi.org/10.1016/j.heliyon.2024.e32371

Alrobaian, S., Alshahrani, S., & Almaleh, A. (2023). Cybersecurity awareness assessment among trainees of the Technical and Vocational Training Corporation. Big Data and Cognitive Computing, 7(2), 73. https://doi.org/10.3390/bdcc7020073

An, Q., Hong, W. C. H., Xu, X., Zhang, Y., & Kolletar-Zhu, K. (2022). How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates. International Journal of Information Security, 22, 305–317. https://doi.org/10.1007/s10207-022-00637-z

Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall.

Barruga, M. B., & Palaoag, T. D. (2025). Cybersecurity strategy for higher education institutions: A thematic analysis on standards and frameworks. Journal of Information Systems Engineering and Management, 10(43s). https://jisem-journal.com/index.php/journal/article/view/8533

Blancaflor, E. B., Castillo, E. C. P., Coretico, J. M. N., Rubiano, G. B., & Tobias, A. M. D. (2023). Philippines' free Wi-Fi roll-out project: Safe or not? Journal of Advances in Information Technology. https://www.jait.us/uploadfile/2023/JAIT-V14N1-20.pdf

Booc, N. B. B., Budiongan, K., & Carballo, R. (2024). Cybersecurity awareness and cybersecurity behavior of high school students in Davao City: A mediation role of perceived behavioral control. European Journal of Applied Science, Engineering and Technology, 2(3), 4–9. https://ejaset.com/index.php/journal/article/view/49

Concepcion, J. D., & Palaoag, T. D. (2024). An assessment of cybersecurity awareness among academic employees at Quirino State University: Promoting cyber hygiene. Journal of Electrical Systems, 20(7s), 769–775. https://journal.esrgroups.org/jes/article/view/3445

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. https://doi.org/10.46382/MJBAS.2024.8216

De Ramos, N. M., & Esponilla, F. D., II. (2024). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education. https://ijere.iaescore.com/index.php/IJERE/article/view/22863

Espiritu, P. G. G., & Jocson, J. C. (2023). Navigating cybersecurity challenges in the era of digital transformation: Threats and mitigation strategies in the Philippines. International Journal of Progressive Research in Science and Engineering, 4(11), 10–23. https://journal.ijprse.com/index.php/ijprse/article/view/994

Gamez-Guadix, M., Fremouw, W., et al. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: A cross sectional study. Crime Science. https://doi.org/10.1186/s40163-024-00230-w

Mahinay, C. J. D., & Mamasalagat, M. P. (2025). Assessing cybercrime awareness and experiences among netizens: A study on the impact of R.A. 10175 in Pagadian City. International Journal of Research and Innovation in Social Science. https://doi.org/10.47772/IJRISS.2025.905000216

Oducado, R. M. F., Dinero, E. M., Fuentes, I. K. M., De la Peña, J. F. L., & Ermita, G. B. (2022). Cybersecurity skills of Filipino nursing students in a public tertiary institution. WVSU Research Journal. https://journal.wvsu.edu.ph/index.php/journals/article/view/90

Republic Act No. 10175. (2012). Cybercrime prevention act of 2012. https://ldr.senate.gov.ph/legislative%2Bissuances/Republic%20Act%20No.%2010175

Republic Act No. 10173. (2012). Data privacy act of 2012. https://www.privacy.gov.ph/data-privacy-act/

Republic Act No. 8792. (2000). Electronic commerce act of 2000. https://pidswebs.pids.gov.ph/CDN/document/pidsbk2023-DigitalEconomy.pdf

Republic Act No. 11967. (2023). Internet transactions act of 2023. https://lawphil.net/statutes/repacts/ra2023/ra_11967_2023.html

Republic Act No. 11927. (2022). Philippine digital workforce competitiveness act. https://lawphil.net/statutes/repacts/ra2022/ra_11927_2022.html

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153–176). Guilford Press.

Saeed, S. (2023). Education, online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. Sustainability, 15(12), 9426. https://doi.org/10.3390/su15129426

Shahrani, S. B., Paizi, W. F., Ariffin, K. A. Z., Othman, Z. A., & Zainudin, S. (2021). Descriptive analysis: The impact of online cyber awareness workshop on teenagers' knowledge of cyber issues. MyJICT. https://myjict.uis.edu.my/index.php/journal/article/download/81/51/123

Snider, K. L. G. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. Journal of Cybersecurity, 7(1), Article tyab019. https://doi.org/10.1093/cybsec/tyab019

Spears, R., & Lea, M. (1994). Panacea or panopticon? The hidden power in computer-mediated communication. Communication Research, 21(4), 427–459.

Tóth, R., Dubniczky, R. A., Limonova, O., & Tihanyi, N. (2025). Sustaining cyber awareness: The long-term impact of continuous phishing training and emotional triggers. arXiv. https://arxiv.org/abs/2510.27298

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540

Vogels, E. A., Gelles-Watnick, R., & Massarat, N. (2022). Teens, social media and technology 2022. Pew Research Center. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/