Impact of Cybersecurity Awareness on the Online Behavior of Residents in Barangay Batasan Hills, Quezon City: A Case Study

Jolina Mae B. Catap, Harold R. Lucero, Reynalyn Mae G. Dela Cruz, Diane Nicole F. Panes, John Ryan Perez, Katrina I. Serzo

College of Computer Studies, Quezon City University

DOI: https://doi.org/10.51244/IJRSI.2026.1305000184

Received: 14 May 2026; Accepted: 19 May 2026; Published: 08 June 2026

ABSTRACT

This study examined the impact of cybersecurity awareness on the online behavior of residents in Barangay Batasan Hills, Quezon City, specifically focusing on their level of awareness, online practices, and ability to recognize cyber risks. A descriptive-quantitative research design was used, and data were gathered from 399 respondents through a researcher-made survey questionnaire using purposive sampling. Results were analyzed using frequency, percentage, and weighted mean. Findings revealed that respondents generally demonstrated a high level of cybersecurity awareness and safe online behavior, with an overall weighted mean of 3.98, interpreted as "Often." Respondents showed strong practices in handling pop-up advertisements and online shopping, both interpreted as "Always," while also demonstrating generally positive behaviors in password management, privacy protection, external link handling, email safety, public Wi-Fi usage, and response to online threats. In terms of awareness, respondents showed a good understanding of cybersecurity threats and online risks, indicating responsible digital engagement. However, weaker areas were identified in password management consistency and phishing identification skills, suggesting a gap between awareness and actual practice. Overall, the findings indicate that cybersecurity awareness significantly influences the online behavior of residents, although not all knowledge is consistently applied in practice. The study concludes that while residents generally practice safe online behavior, continuous cybersecurity education and community-based awareness programs are still necessary to strengthen weak areas such as password security and phishing detection, and to further enhance safe and responsible internet use within the community.

Keywords: Community-based Awareness, Cybersecurity Awareness, Digital Literacy, Online Behavior, Quantitative Research

INTRODUCTION

The rapid advancement of digital technology has significantly transformed the way individuals communicate, access information, and perform daily activities. The widespread use of smartphones, social media platforms, online banking systems, and e-commerce applications has provided greater convenience and accessibility. However, these technological developments have also increased users' exposure to cybersecurity threats such as phishing, identity theft, malware, and online scams. As internet usage continues to expand globally, cybersecurity awareness has become an essential component of digital literacy that promotes safe and responsible online behavior. Recent studies emphasized that individuals with higher levels of cybersecurity awareness are more likely to adopt protective online practices, including creating strong passwords, recognizing suspicious links, and safeguarding personal information while using digital platforms (Zwilling et al., 2022; Hadlington, 2023). Furthermore, cybersecurity awareness has been identified as a critical factor in minimizing user vulnerability and improving decision-making when interacting within digital environments (Department of Information and Communications Technology [DICT], 2024).

In community settings, residents increasingly depend on digital technologies for communication, online transactions, education, entertainment, and access to government services. Despite the benefits of digital connectivity, varying levels of digital literacy and technological exposure may influence how individuals practice online safety and security. Studies conducted in community environments revealed that many residents

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

still lack sufficient knowledge regarding cyber safety practices, resulting in unsafe online behaviors such as sharing sensitive information, using weak passwords, and accessing unsecured networks (Limson et al., 2023). Public awareness initiatives also highlighted the growing need for localized cybersecurity education programs to help residents better understand online risks and adopt safer digital practices (University of the Philippines Open University [UPOU], 2023). These findings suggest that although digital platform usage continues to increase, cybersecurity awareness and online safety practices among community residents remain inconsistent.

In the Philippine context, cybersecurity incidents continue to rise due to the limited knowledge of internet users regarding online safety and preventive cybersecurity measures. Reports from national agencies emphasized that individuals remain vulnerable to cyber threats, particularly phishing attacks, online fraud, and identity theft, because of insufficient awareness and lack of protective practices (DICT, 2024). Community-based studies further revealed that residents often rely heavily on social media and messaging applications without fully understanding the associated risks, thereby increasing their exposure to cybercrime and other digital threats (Limson et al., 2023). These concerns highlight the importance of strengthening cybersecurity awareness among community residents to encourage safer online behavior and reduce cyber-related incidents.

Barangay Batasan Hills, Quezon City, is one of the most populated communities in the city, where residents actively utilize digital technologies for communication, online transactions, education, and access to various services. The large population and widespread internet usage within the barangay increase the likelihood of exposure to cybersecurity risks among residents (PhilAtlas, 2023). A study conducted in Barangay Batasan Hills reported incidents involving identity theft and misuse of personal information, indicating the need to improve cybersecurity awareness and promote safe online practices among community members (Tura et al., 2024). Additionally, studies conducted in barangay communities emphasized that residents often lack sufficient awareness of cybersecurity threats, making them vulnerable to phishing attacks, scams, and other online risks (Limson et al., 2023). Despite these findings, limited localized studies have specifically examined how cybersecurity awareness influences the online behavior of residents at the barangay level, particularly in Barangay Batasan Hills, Quezon City.

This research gap highlights the need to investigate cybersecurity awareness and its impact on the online behavior of residents in Barangay Batasan Hills. Understanding the residents' level of cybersecurity awareness and their online practices may provide valuable insights into potential vulnerabilities within the community. By identifying existing awareness levels and online behaviors, appropriate interventions and educational programs may be developed to promote safer online practices and strengthen community-based digital safety initiatives.

This study aims to determine the impact of cybersecurity awareness on the online behavior of residents in Barangay Batasan Hills, Quezon City. Specifically, it seeks to assess the level of cybersecurity awareness among residents, identify their online behavior when using digital technologies, and determine the relationship between cybersecurity awareness and online behavior. The findings of this study may serve as a basis for developing community-based cybersecurity awareness programs and educational initiatives tailored to the needs of residents.

The results of this study are expected to benefit community residents, barangay officials, and local government units by providing baseline information regarding cybersecurity awareness within the community. The findings may support the implementation of targeted awareness campaigns and digital safety programs aimed at reducing cybersecurity risks and promoting responsible internet usage. Furthermore, this study contributes to the existing body of literature by addressing the gap in community-level cybersecurity awareness research and providing insights into the online behavior of residents in Barangay Batasan Hills, Quezon City.

A. Statement of the Problem

The increasing reliance on digital technologies among residents of Barangay Batasan Hills, Quezon City has exposed individuals to various cybersecurity threats such as phishing, identity theft, and online scams. Despite the growing use of online platforms for communication, transactions, and access to services, cybersecurity awareness among community residents remains inconsistent. This situation may influence how individuals

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

behave online, potentially increasing their vulnerability to cyber risks. Thus, this study aims to examine the impact of cybersecurity awareness on the online behavior of residents in Barangay Batasan Hills, Quezon City.

Specifically, it seeks to answer the following questions:

1. How often the residents check their cybersecurity awareness in terms of:

a. Changing Password

b. Privacy Settings

c. External Links

d. Anonymous Email

e. Pop-Up Ads

f. Public Wifis

g. Chatting to Strangers

h. Online Shopping

2. What is the level of online behavior of residents in terms of:

a. Safe browsing practices

b. Protection of personal information

c. Response to suspicious online threats

3. What is the level of cybersecurity awareness of the residents in terms of:

a. Knowledge of cybersecurity threats

b. Awareness in online shopping/safe online practices

c. Ability to recognize online risks

Related Studies

Cybersecurity awareness has consistently been identified in both international and local literature as a significant factor influencing individuals' online behavior. Studies revealed that individuals with greater knowledge of cybersecurity concepts are more likely to practice safe online behaviors, such as creating strong passwords, identifying phishing attempts, protecting personal information, and avoiding suspicious online activities. Research conducted by Lee and Chua (2023), Musaddag Elrayah and Jamil (2023), and Zwilling et al. (2022) emphasized that cybersecurity awareness contributes to responsible digital behavior, particularly when combined with broader digital literacy competencies. These studies collectively suggest that cybersecurity awareness serves as a foundation for secure online practices by enabling individuals to recognize potential cyber threats and apply appropriate protective measures while using digital technologies.

Despite the positive relationship between cybersecurity awareness and online safety practices, several studies identified the existence of a knowledge-behavior gap, wherein individuals possess cybersecurity knowledge but fail to consistently apply it in actual online situations. Bognár and Bottyán (2024), Khan et al. (2022), and Rotas and Cahapay (2021) found that many users demonstrate awareness of cybersecurity risks yet still engage in unsafe online behaviors due to convenience, negligence, overconfidence, and habitual internet use. Similar findings were observed in Philippine-based studies conducted by De Guzman and Rivera (2024), Escobar

(2022), and Alabab et al. (2024), which revealed that although respondents were aware of cybersecurity threats and preventive measures, the practical application of such knowledge remained inconsistent. These findings indicate that awareness alone is insufficient to ensure secure online behavior, highlighting the need for strategies that reinforce the consistent practice of cybersecurity measures.

The literature further emphasized that cybersecurity behavior is influenced not only by awareness but also by psychological, social, and demographic factors. Alanazi, Freeman, and Tootell (2022) explained that attitudes, subjective norms, and perceived behavioral control significantly influence individuals' cybersecurity intentions and actual practices. Likewise, Debb and McClellan (2021) noted that perceived vulnerability to cyber threats motivates individuals to adopt protective online behaviors. Social influence also emerged as a significant determinant of cybersecurity behavior. Hong et al. (2023) found that peer behaviors and social environments often shape cybersecurity practices more strongly than individual knowledge alone. In the local context, Loyola et al. (2026) and Booc et al. (2024) similarly revealed that factors such as age, confidence in using technology, and level of exposure to digital platforms influence cybersecurity awareness and online behavior among users. These findings suggest that cybersecurity behavior is multidimensional and shaped by both personal and environmental factors.

Moreover, the reviewed studies highlighted the importance of continuous and structured cybersecurity education in strengthening safe online practices. International studies recommended integrating cybersecurity awareness programs into educational systems and broader digital literacy initiatives to address the gap between knowledge and actual behavior. This perspective is supported by local studies conducted by Cuares and Casaña (2026), Dapitan et al. (2024), and Toso et al. (2023), which emphasized that regular reinforcement, targeted training programs, and curriculum integration are essential in developing practical cybersecurity skills and improving online safety behavior. Additionally, Pasia (2025) highlighted the value of community-based approaches, emphasizing that collective awareness efforts and collaboration with institutions can further enhance cybersecurity behavior beyond individual initiatives. These findings demonstrate the importance of sustained educational interventions in promoting responsible and secure online practices within communities.

Overall, the reviewed literature demonstrates that cybersecurity awareness significantly influences online behavior; however, its effectiveness is shaped by several interconnected factors, including behavioral intention, social influence, perceived risk, technological exposure, and practical experience. Both foreign and local studies consistently emphasized the need for comprehensive and behavior-focused cybersecurity education programs that extend beyond knowledge acquisition. The literature further suggests that effective cybersecurity behavior requires continuous reinforcement and strategies that address not only awareness but also the behavioral and social factors influencing how individuals act within digital environments. These findings support the present study by establishing the importance of examining cybersecurity awareness and online behavior at the community level, particularly among residents in Barangay Batasan Hills, Quezon City.

METHODOLOGY

A. Research Design

This study employed a descriptive-quantitative research design to examine the impact of cybersecurity awareness on the online behavior of residents in Barangay Batasan Hills, Quezon City. The descriptive-quantitative design was deemed appropriate because it enables the researchers to systematically describe, measure, and analyze the current level of cybersecurity awareness and online behavior among community residents using numerical data. Through this approach, the researchers were able to objectively assess the frequency of cybersecurity practices, the level of cybersecurity awareness, and the respondents' online behaviors when using digital technologies.

This research design has been widely utilized in similar cybersecurity-related studies, particularly those conducted by Lee and Chua (2023), De Guzman and Rivera (2024), and Ahamed et al. (2026), which also focused on assessing and describing cybersecurity awareness and online behavior among community-based populations. The use of a quantitative approach further allowed the researchers to analyze the collected data

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

using statistical methods and determine patterns and trends related to cybersecurity awareness and online practices.

A total of 399 respondents participated in the study to ensure adequate sample representation and obtain statistically reliable results with a minimal margin of error.

B. Data Gathering

Population and Sampling

The respondents of this study were residents of Barangay Batasan Hills, Quezon City, which has a recorded population of 168,770 based on the 2024 POPCEN (Census of Population). To determine the required sample size, the researchers applied Slovin's Formula:

$$\boldsymbol{n = \frac{N}{1+Ne^2}}$$

Where:

n = sample size

N = total population

e = margin of error

Using a 5% margin of error (e=0.05), the computed sample size resulted in 399 respondents.

The respondents were selected through purposive sampling. The primary criterion for participation was that the respondents must be residents of Barangay Batasan Hills, Quezon City, and active users of digital technologies or social media platforms. No specific age bracket was imposed in order to obtain responses from internet users belonging to different age groups within the community.

Data Gathering Tools

The researchers used a researcher-made survey questionnaire as the primary data gathering instrument for the study. The questionnaire was designed to assess the cybersecurity awareness and online behavior of residents in Barangay Batasan Hills, Quezon City. The instrument consisted of four major sections:

a. **Technical Habits** – focused on password management and privacy settings;

b. **Web Safety** – examined respondents' behavior in handling links, emails, and public Wi-Fi networks;

c. **Consumer Awareness** – assessed online shopping and financial security practices; and

d. **Cognitive Awareness** – evaluated respondents' knowledge regarding phishing, malware, and other cybersecurity threats.

The questionnaire utilized a 5-point Likert Scale to measure the respondents' answers. Two rating scales were used depending on the nature of the survey items.

Table 1 5-Point Likert Scale Used for Cybersecurity Practices

Score	Interpretation
5	Always

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

4	Often
3	Sometimes
2	Rarely
1	Never

Table 2 5-Point Likert Scale Used for Cybersecurity Awareness

Score	Interpretation
5	Strongly Agree (SA)
4	Agree (A)
3	Neutral (N)
2	Disagree (D)
1	Strongly Disagree (SD)

Prior to the actual data collection, the questionnaire was validated by the research adviser and subject experts to ensure the clarity, relevance, and appropriateness of the survey items.

Data Gathering Procedure

Prior to conducting the study, the researchers secured permission from the appropriate authorities and obtained the consent of the respondents to ensure ethical compliance and proper coordination throughout the research process.

Data collection was conducted using two modes of survey administration. The primary method involved the distribution of an online survey questionnaire through Google Forms, which enabled efficient and wide-reaching participation among residents with internet access and smartphones.

For respondents who had limited access to mobile devices or internet connectivity, particularly middle-aged and older residents, the researchers employed a researcher-assisted survey approach. In this process, the researchers personally read the survey questions aloud and recorded the respondents' answers on their behalf. This dual-mode data collection approach ensured inclusivity and prevented the exclusion of participants due to technological limitations.

After all responses were collected, the data were organized, tabulated, analyzed, and interpreted using appropriate statistical tools.

C. Statistical Treatment of Data

The data gathered from the survey questionnaires were processed and analyzed using appropriate statistical tools to address the objectives of the study. The following statistical measures were utilized:

Frequency and Percentage

Frequency and percentage were used to describe the demographic profile of the respondents and summarize the distribution of responses across the survey items.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Weighted Mean

The weighted mean was used to determine the average response for each survey item and to measure the overall level of cybersecurity awareness and online behavior among the respondents. The formula used is shown below:

$$WM = \frac{\Sigma(f \times w)}{N}$$

Where:

WM= weighted mean

f = frequency of responses

w = weight assigned to each response

N = total number of respondents

Verbal Interpretation

The computed weighted means were interpreted using an appropriate verbal interpretation scale to categorize the level of cybersecurity awareness and online behavior of the respondents.

RESULT AND DISCUSSION

This chapter presents the data gathered through research instruments. This section aims to analyze and interpret the collected data based on the respondents' answers and relate them to the objectives of the study. Through this analysis, the study provides insights and conclusions that support the overall purpose of the research.

Profile of the Respondents

Table 3 Demographic Profile of the Respondents According to Age and Gender

DEMOGRAPHIC VARIABLE	CATEGORY	FREQUENCY	PERCENTAGE
Age	17 years old and below	28	7.00%
	18 – 24	83	20.8%
	25 – 34	76	19.00%
	35 – 44	65	16.30%
	45 – 54	58	14.50%
	55 – 64	49	12.30%
	65 years old and older	40	10.00%
	Total	**399**	**100.00%**
Gender	Male	198	49.50%
	Female	181	45.30%
	Prefer not to say	18	4.50%

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

	Others	2	0.50%
	Total	**399**	**100.00%**

Table 3 presents the demographic profile of the respondents according to age and gender. The majority of the respondents belonged to the 18–24 years old age group with a frequency of 83 or 20.8%, while most respondents were male with a frequency of 198 or 49.6% of the total 399 respondents. The findings indicate that the study gathered responses from residents with diverse demographic backgrounds regarding cybersecurity awareness and online behavior.

Degree of Cybersecurity Practices Among Residents

Passwords Management

Table 4 Respondent's Assessment of their Password Management Practices

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I change my passwords regularly	47	75	132	122	23	3.00	Sometimes
I create strong passwords for my accounts	156	101	104	28	10	3.91	Often
I avoid reusing the same password on multiple accounts	74	89	141	69	26	3.91	Often
Overall Mean						**3.61**	**Often**

Table 4 presents the respondents' assessment regarding their password management practices. The table shows an overall weighted mean of 3.61, verbally interpreted as "Often," indicating that the respondents generally practice proper password security measures in their online accounts. The statements "I create strong passwords for my accounts" and "I avoid reusing the same password on multiple accounts" both obtained a weighted mean of 3.91, interpreted as "Often." These findings suggest that respondents are aware of the importance of using strong and unique passwords to protect their online accounts from unauthorized access and cyber threats.

Meanwhile, the statement "I change my passwords regularly" obtained the lowest weighted mean of 3.00, verbally interpreted as "Sometimes." This indicates that although respondents practice creating strong and unique passwords, they do not consistently update their passwords regularly. The result suggests a need to further strengthen cybersecurity awareness programs emphasizing the importance of regular password changes as part of safe online behavior.

Privacy Settings and Account Management

Table 5 Respondent's Assessment of their Privacy and Account Management Practices

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I review my privacy settings on social media accounts	111	119	117	49	12	3.69	Often

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

I limit who can view my personal information online	139	126	96	31	7	3.90	Often
I update my account privacy settings when needed	135	107	104	44	9	3.90	Often
Overall Mean						**3.83**	**Often**

Table 5 presents the respondents' assessment of their privacy and account management practices. The table obtained an overall weighted mean of 3.83, verbally interpreted as "Often," indicating that the respondents generally practice proper privacy management in their online accounts. Among the indicators, the statements "I limit who can view my personal information online" and "I update my account privacy settings when needed" both received the highest weighted mean of 3.90, interpreted as "Often." This suggests that respondents are generally aware of the importance of protecting personal information and maintaining updated privacy settings to reduce online risks. Meanwhile, the statement "I review my privacy settings on social media accounts" obtained the lowest weighted mean of 3.69, although still verbally interpreted as "Often." Overall, the findings imply that respondents demonstrate positive online privacy management practices, reflecting a relatively good level of cybersecurity awareness regarding the protection of personal information online.

External Links

Table 6 below shows the respondents' assessment of their practices in handling external links. The table obtained an overall weighted mean of 4.06, verbally interpreted as "Often," indicating that the respondents generally practice caution when dealing with online links and websites. Among the indicators, the statement "I avoid clicking links from unknown sources" received the highest weighted mean of 4.17, interpreted as "Often," suggesting that respondents are highly aware of the risks associated with suspicious or unfamiliar links. Similarly, the statement "I check if a link is safe before clicking it" obtained a weighted mean of 4.07, while "I verify website URLs before entering information" garnered the lowest weighted mean of 3.95, though still interpreted as "Often." Overall, the findings indicate that respondents commonly practice safe behaviors when handling external links, reflecting a good level of cybersecurity awareness in protecting themselves from phishing attacks, scams, and malicious websites.

Table 6 Respondent's Assessment of their Practices in Handling External Links

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I check if a link is safe before clicking it	481	107	81	24	6	4.07	Often
I avoid clicking links from unknown sources	195	116	57	23	8	4.17	Often
I verify website URLs before entering information	163	100	102	23	11	3.95	Often
Overall Mean						**4.06**	**Often**

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Anonymous Email

Table 7 Respondent's Assessment of their Anonymous Email Handling Practices

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I check the sender's identity before opening emails	167	119	85	22	6	4.05	Often
I avoid replying to suspicious emails	196	117	56	25	5	4.19	Often
I delete anonymous emails immediately	148	111	93	38	9	3.88	Often
Overall Mean						**4.04**	**Often**

Table 7 illustrates the respondents' assessment of their anonymous email handling practices. The table obtained an overall weighted mean of 4.04, verbally interpreted as "Often," indicating that the respondents generally practice caution when dealing with suspicious or anonymous emails. Among the indicators, the statement "I avoid replying to suspicious emails" received the highest weighted mean of 4.19, interpreted as "Often," suggesting that respondents are highly aware of the potential risks associated with fraudulent or malicious emails. The statement "I check the sender's identity before opening emails" also obtained a high weighted mean of 4.05, while "I delete anonymous emails immediately" received the lowest weighted mean of 3.88, though still verbally interpreted as "Often." Overall, the findings indicate that respondents commonly practice safe email handling behaviors, reflecting a good level of cybersecurity awareness in protecting themselves from phishing attempts, scams, and other email-related cyber threats.

Popo-up Advertisements

Table 8 Respondent's Assessment of their Practices Regarding Pop-p Ads

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I avoid clicking on suspicious pop-up ads	210	101	67	14	7	4.24	Always
I close unwanted pop-up windows immediately	213	103	56	22	5	4.25	Always
I avoid downloading files from pop-up ads	201	96	75	20	7	4.16	Often
Overall Mean						**4.22**	**Always**

Table 8 presents the respondents' assessment of their practices regarding pop-up advertisements. The table obtained an overall weighted mean of 4.22, verbally interpreted as "Always," indicating that the respondents consistently practice safe behaviors when encountering suspicious pop-up ads online. Among the indicators, the statement "I close unwanted pop-up windows immediately" received the highest weighted mean of 4.25,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

interpreted as "Always," followed closely by "I avoid clicking on suspicious pop-up ads" with a weighted mean of 4.24. Meanwhile, the statement "I avoid downloading files from pop-up ads" obtained the lowest weighted mean of 4.16, although it was still verbally interpreted as "Often." Overall, the findings suggest that respondents demonstrate a high level of cybersecurity awareness and caution in handling pop-up advertisements, which may help reduce their exposure to malware, scams, and other online threats.

Public Wi-Fi Usage

Table 9 Respondent's Assessment of their Practices in Public Wi-Fi Usage

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I avoid connecting to unsecured public Wi-Fi?	154	123	101	14	7	4.01	Often
I use secure connections when using public Wi-Fi	212	103	56	22	6	4.24	Always
I avoid accessing into sensitive accounts on public Wi-F	201	96	75	20	7	4.16	Often
Overall Mean						**4.22**	**Always**

Table 9 displays the respondents' assessment of their practices regarding the use of public Wi-Fi networks. The table obtained an overall weighted mean of 4.22, verbally interpreted as "Always," indicating that the respondents consistently practice safe behaviors when using public internet connections. Among the indicators, the statement "I use secure connections when using public Wi-Fi" received the highest weighted mean of 4.24, interpreted as "Always," suggesting that respondents are highly aware of the importance of securing their internet connection in public environments. Meanwhile, the statements "I avoid accessing sensitive accounts on public Wi-Fi" and "I avoid connecting to unsecured public Wi-Fi" obtained weighted means of 4.16 and 4.01, respectively, both interpreted as "Often." Overall, the findings indicate that respondents generally demonstrate responsible and secure practices when using public Wi-Fi, reflecting a good level of cybersecurity awareness in protecting personal and sensitive information from potential cyber threats.

Chatting to Stranger

Table 10 Respondent's Assessment of their Practices in Regarding Chatting to Strangers

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I avoid sharing personal information with strangers online	196	105	68	21	9	4.15	Often
I block suspicious strangers who contact me	212	103	56	22	6	4.24	Always

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

I stay cautious when chatting with strangers online	189	102	75	23	10	4.10	Often
Overall Mean						**4.16**	**Always**

Table 10 exhibits the respondents' assessment of their practices regarding communicating with strangers online. The table obtained an overall weighted mean of 4.16, verbally interpreted as "Always," indicating that the respondents consistently practice caution and safety when interacting with unfamiliar individuals online. Among the indicators, the statement "I block suspicious strangers who contact me" received the highest weighted mean of 4.24, interpreted as "Always," suggesting that respondents actively protect themselves from potentially harmful or suspicious online interactions. Meanwhile, the statements "I avoid sharing personal information with strangers online" and "I stay cautious when chatting with strangers online" obtained weighted means of 4.15 and 4.10, respectively, both verbally interpreted as "Often." Overall, the findings indicate that respondents generally demonstrate responsible online communication practices, reflecting a high level of cybersecurity awareness in protecting themselves from scams, identity theft, and other online threats associated with interacting with strangers.

Online Shopping

Table 11 below, shows the respondents' assessment of their practices regarding online shopping. The table obtained an overall weighted mean of 4.22, verbally interpreted as "Always," indicating that the respondents consistently practice safe and responsible behaviors when engaging in online shopping activities. Among the indicators, the statement "I read reviews before purchasing online" received the highest weighted mean of 4.27, interpreted as "Always," suggesting that respondents commonly verify the credibility and reliability of products or sellers before making purchases. Similarly, the statement "I check if a shopping platform is secure before buying" obtained a weighted mean of 4.23, while "I avoid sharing payment details on suspicious platforms" received the lowest weighted mean of 4.17, though still verbally interpreted as "Often." Overall, the findings indicate that respondents demonstrate a high level of cybersecurity awareness in online shopping, particularly in verifying platform security and avoiding suspicious transactions to protect their personal and financial information.

Table 11Respondent's Assessment of their Practices in Regarding Online Shopping

Question	5 (Always)	4 (Often)	3 (Sometimes)	2 (Rarely)	1 (Never)	Weighted Mean	Verbal Interpretation
I check if a shopping platform is secure before buying	209	106	56	22	6	4.23	Always
I read reviews before purchasing online	220	99	53	21	6	4.27	Always
I avoid sharing payment details on suspicious platforms	202	97	72	21	7	4.17	Often
Overall Mean						**4.22**	**Always**

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Summary

Table 12 Respondent's Assessment of their Cybersecurity Awareness Across All Indicators

Indicators	Weighted Mean	Verbal Interpretation
Passwords Management	3.61	Often
Privacy Settings	3.83	Often
External Links	4.06	Often
Anonymous Email	4.04	Often
Pop-up Advertisements	4.24	Always
Public Wi-Fi	4.14	Often
Chatting to Strangers	4.16	Often
Online Shopping	4.22	Always
Overall Weighted Mean	**3.98**	**Often**

Table 12 presents the respondents' overall assessment of their online behavior across different cybersecurity-related practices. The table obtained an overall weighted mean of 3.98, verbally interpreted as "Often," indicating that the respondents generally practice safe and responsible online behaviors in their daily use of digital technologies. Among the indicators, "Pop-up Advertisements" obtained the highest weighted mean of 4.24, verbally interpreted as "Always," followed closely by "Online Shopping" with a weighted mean of 4.22. These findings suggest that respondents consistently practice caution when dealing with suspicious advertisements and online shopping activities. Meanwhile, "Password Management" obtained the lowest weighted mean of 3.61, although still interpreted as "Often," indicating that password-related security practices are less consistently observed compared to other cybersecurity behaviors.

Overall, the findings indicate that the respondents demonstrate a relatively good level of cybersecurity awareness and online safety practices, particularly in handling online transactions, suspicious advertisements, and external online interactions. However, the lower result in password management suggests the need for further awareness initiatives and educational programs emphasizing the importance of maintaining strong and regularly updated passwords as part of effective cybersecurity behavior.

Resident's Level of Online Behaviors

Safe Browsing Practices

Table 13 Respondent's Assessment of their Safe Browsing Practices

Question	5 (SA)	4 (A)	3 (N)	2 (D)	1 (SD)	Weighted Mean	Verbal Interpretation
I only visit secure and trusted websites when browsing online.	177	124	73	16	9	4.11	Agree

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

I avoid clicking on unknown or suspicious links.	206	118	51	18	6	4.25	Strongly Agree
I regularly update my browser and applications for security.	158	120	87	28	6	3.99	Agree
I check website URLs to ensure they are legitimate before entering information.	162	124	86	22	5	4.04	Agree
Overall Mean						**4.10**	**Agree**

Table 13 presents the respondents' assessment of their safe browsing practices. The table obtained an overall weighted mean of 4.10, verbally interpreted as "Agree," indicating that the respondents generally practice safe and secure browsing behaviors when using the internet. Among the indicators, the statement "I avoid clicking on unknown or suspicious links" received the highest weighted mean of 4.25, verbally interpreted as "Strongly Agree," suggesting that respondents are highly cautious when encountering potentially harmful links online. Meanwhile, the statement "I regularly update my browser and applications for security" obtained the lowest weighted mean of 3.99, although still verbally interpreted as "Agree." The remaining indicators, including visiting secure websites and verifying website URLs before entering information, also received positive assessments from the respondents. Overall, the findings indicate that respondents demonstrate a good level of cybersecurity awareness in practicing safe browsing behaviors to protect themselves from online threats such as phishing, malware, and fraudulent websites.

Online Protections of Personal Information

Table 14 Respondent's Assessment Regarding their Protection of Personal Information Online

Question	5 (SA)	4 (A)	3 (N)	2 (D)	1 (SD)	Weighted Mean	Verbal Interpretation
I avoid sharing personal information on social media platforms. (e.g., Facebook, Twitter, Instagram, and online forums)	179	137	66	10	7	4.18	Agree
I use strong and unique passwords for my online accounts.	180	133	61	17	8	4.15	Agree
I enable privacy settings on my social media accounts.	179	128	67	21	4	4.15	Agree
I do not save sensitive information on shared or public devices.	182	131	59	22	5	4.16	Agree
Overall Mean						**4.16**	**Agree**

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Table 14 presents the respondents' assessment regarding their protection of personal information online. The table obtained an overall weighted mean of 4.16, verbally interpreted as "Agree," indicating that the respondents generally practice responsible behaviors in protecting their personal information while using online platforms and digital technologies. Among the indicators, the statement "I avoid sharing personal information on social media platforms" received the highest weighted mean of 4.18, suggesting that respondents are cautious in disclosing sensitive information on social networking sites and online forums. The statements "I do not save sensitive information on shared or public devices," "I use strong and unique passwords for my online accounts," and "I enable privacy settings on my social media accounts" also obtained high weighted means of 4.16 and 4.15, respectively, all verbally interpreted as "Agree." Overall, the findings indicate that respondents demonstrate a good level of cybersecurity awareness and practice preventive measures to safeguard their personal information from potential online threats and privacy risks.

Response to Online Threats

Table 15 Respondent's Assessment Regarding their Response to Online Threats

Question	5 (SA)	4 (A)	3 (N)	2 (D)	1 (SD)	Weighted Mean	Verbal Interpretation
I ignore suspicious emails or messages.	182	130	73	11	3	4.20	Agree
I report suspicious accounts, links, or messages when I encounter them.	164	122	93	17	3	4.07	Agree
I verify the source before responding to unexpected online requests.	172	128	82	14	3	4.13	Agree
I avoid downloading files from untrusted sources.	165	143	67	18	6	4.11	Agree
Overall Mean						**4.13**	**Agree**

Table 15 presents the respondents' assessment regarding their response to online threats. The table obtained an overall weighted mean of 4.13, verbally interpreted as "Agree," indicating that the respondents generally practice appropriate and cautious responses when encountering potential cybersecurity threats online. Among the indicators, the statement "I ignore suspicious emails or messages" received the highest weighted mean of 4.20, suggesting that respondents are highly cautious in dealing with potentially harmful communications. Meanwhile, the statements "I verify the source before responding to unexpected online requests," "I avoid downloading files from untrusted sources," and "I report suspicious accounts, links, or messages when I encounter them" obtained weighted means of 4.13, 4.11, and 4.07, respectively, all verbally interpreted as "Agree." Overall, the findings indicate that respondents demonstrate a good level of cybersecurity awareness and apply preventive measures to protect themselves from phishing attempts, scams, malware, and other online threats.

Resident's Level of Cybersecurity Awareness

Knowledge of Cybersecurity Threats

Table 16 Respondent's Assessment of their Knowledge of Cybersecurity Threats

Question	5 (SA)	4 (A)	3 (N)	2 (D)	1 (SD)	Weighted Mean	Verbal Interpretation
I am familiar with common cybersecurity	170	114	82	17	16	4.02	Agree

threats such as phishing, malware, and scams.							
I understand how cyberattacks can affect my personal information.	189	116	60	20	14	4.12	Agree
I can identify signs of a phishing email or message.	148	115	94	24	18	3.88	Agree
Overall Mean						**4.01**	**Agree**

Table 16 presents the respondents' assessment of their knowledge of cybersecurity threats. The table obtained an overall weighted mean of 4.01, verbally interpreted as "Agree," indicating that the respondents generally possess a good level of awareness regarding common cybersecurity threats and their possible effects. Among the indicators, the statement "I understand how cyberattacks can affect my personal information" received the highest weighted mean of 4.12, suggesting that respondents are aware of the risks cyberattacks pose to their privacy and security. Meanwhile, the statement "I am familiar with common cybersecurity threats such as phishing, malware, and scams" obtained a weighted mean of 4.02, while "I can identify signs of a phishing email or message" received the lowest weighted mean of 3.88, although still verbally interpreted as "Agree." Overall, the findings indicate that respondents demonstrate a relatively good understanding of cybersecurity threats; however, the lower result in identifying phishing attempts suggests a need for additional awareness programs and training focused on recognizing suspicious emails and online scams.

Awareness in Online Shopping /Safe Browsing Practices

Table 17 Respondent's Assessment of their Online Shopping/Safe Browsing Practices

Question	5 (SA)	4 (A)	3 (N)	2 (D)	1 (SD)	Weighted Mean	Verbal Interpretation
I check if an online store is legitimate before making a purchase.	180	135	68	11	5	4.19	Agree
I use secure payment methods when shopping online.	193	128	63	11	4	4.24	Strongly Agree
I read reviews or ratings before buying products online.	198	110	76	12	3	4.22	Strongly Agree
I avoid sharing financial information on unsecured websites.	187	125	64	19	4	4.18	Agree
Overall Mean						**4.21**	**Strongly Agree**

Table 17 exhibits the respondents' assessment of their online shopping and safe browsing practices. The table obtained an overall weighted mean of 4.21, verbally interpreted as "Strongly Agree," indicating that the respondents consistently practice safe and responsible behaviors when engaging in online shopping and browsing activities. Among the indicators, the statement "I use secure payment methods when shopping online" received the highest weighted mean of 4.24, followed closely by "I read reviews or ratings before buying products online" with a weighted mean of 4.22, both verbally interpreted as "Strongly Agree." These findings suggest that respondents are highly cautious when conducting online transactions and actively verify the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

credibility of products and sellers before making purchases. Meanwhile, the statements "I check if an online store is legitimate before making a purchase" and "I avoid sharing financial information on unsecured websites" obtained weighted means of 4.19 and 4.18, respectively, both verbally interpreted as "Agree." Overall, the findings indicate that respondents demonstrate a high level of cybersecurity awareness and safe online shopping practices aimed at protecting their financial and personal information from online threats and fraudulent activities.

Ability to Recognize Online Risks

Table 18 Respondent's Assessment of their Ability to Recognize Online Risks

Question	5 (SA)	4 (A)	3 (N)	2 (D)	1 (SD)	Weighted Mean	Verbal Interpretation
I can identify suspicious links or fake websites.	152	135	88	20	4	4.03	Agree
I am aware of the risks of using public Wi-Fi for sensitive transactions	189	130	59	18	3	4.21	Strongly Agree
I recognize when an online offer or message seems too good to be true.	180	119	78	16	6	4.13	Agree
I can differentiate between legitimate and fake online accounts.	164	138	71	23	3	4.09	Agree
Overall Mean						**4.12**	**Agree**

Table 18 presents the respondents' assessment of their ability to recognize online risks. The table obtained an overall weighted mean of 4.12, verbally interpreted as "Agree," indicating that the respondents generally possess a good level of awareness in identifying potential online threats and suspicious online activities. Among the indicators, the statement "I am aware of the risks of using public Wi-Fi for sensitive transactions" received the highest weighted mean of 4.21, verbally interpreted as "Strongly Agree," suggesting that respondents are highly aware of the security risks associated with public internet connections. Meanwhile, the statements "I recognize when an online offer or message seems too good to be true," "I can differentiate between legitimate and fake online accounts," and "I can identify suspicious links or fake websites" obtained weighted means of 4.13, 4.09, and 4.03, respectively, all verbally interpreted as "Agree." Overall, the findings indicate that respondents demonstrate a relatively strong ability to recognize online risks and potential cyber threats, reflecting a good level of cybersecurity awareness in protecting themselves from scams, phishing attempts, and fraudulent online activities.

CONCLUSION

The findings of the study revealed that the residents of Barangay Batasan Hills, Quezon City generally demonstrate a good level of cybersecurity awareness and responsible online behavior. The respondents commonly practice safe online habits such as avoiding suspicious links and anonymous emails, checking the legitimacy of websites and online stores, using secure payment methods, managing privacy settings, and protecting personal information online. The results further showed that respondents consistently practice caution when encountering pop-up advertisements, using public Wi-Fi connections, and communicating with strangers online. These findings indicate that the residents are aware of common cybersecurity risks and apply preventive measures to protect themselves from cyber threats such as phishing, scams, malware, identity theft, and fraudulent online activities.

The study also revealed that respondents possess a relatively good understanding of cybersecurity threats and online risks. Most respondents agreed that they are familiar with common cybersecurity threats, understand the effects of cyberattacks on personal information, and can recognize suspicious online offers, fake websites, and risky online activities. Additionally, the respondents demonstrated responsible online shopping and safe browsing behaviors by verifying website legitimacy, reading online reviews, and avoiding the sharing of sensitive financial information on unsecured platforms. These findings suggest that cybersecurity awareness among the residents contributes positively to their online decision-making and safety practices when using digital technologies.

Despite the generally positive results, the study identified certain areas that still require improvement. Among all indicators, password management practices obtained comparatively lower assessments, particularly regarding the regular changing of passwords. Similarly, the ability to identify phishing emails and suspicious online messages received lower weighted means compared to other indicators. These findings imply that although respondents are aware of cybersecurity threats, some preventive cybersecurity practices are not always applied consistently in actual online situations. This reflects the presence of a knowledge-practice gap, wherein awareness does not always translate into continuous and effective cybersecurity behavior.

Based on the results presented, the study concludes that cybersecurity awareness plays a significant role in shaping the online behavior of residents in Barangay Batasan Hills, Quezon City. The respondents generally exhibit safe and responsible online practices; however, continuous reinforcement through cybersecurity awareness programs, community-based digital safety initiatives, and educational campaigns remains necessary to further strengthen cybersecurity behavior among residents. It is recommended that barangay officials, local government units, and educational institutions collaborate in conducting regular cybersecurity seminars, workshops, and awareness campaigns focused on practical online safety skills such as password management, phishing detection, privacy protection, and safe internet usage. Community-based training programs and information dissemination activities may further improve residents' cybersecurity awareness and encourage the consistent application of safe online practices. Future researchers may also conduct related studies involving other communities or additional variables to further understand the factors influencing cybersecurity awareness and online behavior.

REFERENCES

1 A. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among users and its impact on security behavior," Computers & Security, vol. 120, p. 102819, 2022. doi: 10.1016/j.cose.2022.102819.
2 Department of Information and Communications Technology, "Cybersecurity awareness initiatives for communities," 2024. [Online]. Available: https://dict.gov.ph. Accessed: Apr. 27, 2026.
3 L. Hadlington, "Human factors in cybersecurity: Examining the link between knowledge and online behavior," Computers & Security, vol. 126, p. 103065, 2023. doi: 10.1016/j.cose.2023.103065.
4 K. R. Limson, D. Avila, N. J. Lota, and D. B. Diaz, "Assessment on the community awareness on cybercrime at Barangay Pasong Tamo, Quezon City," Ascendens Asia Singapore – Bestlink College of the Philippines Journal of Multidisciplinary Research, vol. 4, no. 1, 2023. [Online]. Available: https://ojs.aaresearchindex.com/index.php/aasgbcpjmra/article/view/13944. Accessed: Apr. 27, 2026.
5 PhilAtlas, "Batasan Hills, Quezon City profile and population," 2023. [Online]. Available: https://www.philatlas.com/luzon/ncr/quezon-city/batasan-hills.html. Accessed: Apr. 27, 2026.
6 M. S. Tura et al., "Identity theft awareness in Barangay Batasan Hills, Quezon City: Basis for social media platform safety," Ascendens Asia Singapore – Bestlink College of the Philippines Journal of Multidisciplinary Research, vol. 6, no. 1, 2024. [Online]. Available: https://ojs.aaresearchindex.com/index.php/aasgbcpjmra/article/view/17011. Accessed: Apr. 27, 2026.
7 University of the Philippines Open University, "Cybersecurity awareness month: Building secure communities," 2023. [Online]. Available: https://www.upou.edu.ph/news/cybersecurity-awareness-month-2023-cybersecurity-driven-resilience-building-a-secure-foundation/. Accessed: Apr. 27, 2026.
8 M. Zwilling et al., "Cybersecurity awareness, knowledge and behavior: A comparative study," Journal of Computer Information Systems, vol. 62, no. 1, pp. 82–97, 2022. doi: 10.1080/08874417.2022.1712269.

9 L. Bognár and L. Bottyán, “Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students,” Education Sciences, vol. 14, no. 6, p. 588, 2024, https://www.mdpi.com/2227-7102/14/6/588.
10 M. Elrayah and S. Jamil, “Impact of digital literacy and online privacy concerns on cybersecurity behavior: The moderating role of cybersecurity awareness,” International Journal of Cyber Criminology, vol. 17, no. 2, pp. 166–187, 2023, https://doi.org/10.5281/zenodo.4766711.
11 C. S. Lee and Y. T. Chua, “The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States,” Crime & Delinquency, vol. 70, no. 9, pp. 2250–2277, 2024. The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States - Claire Seungeun Lee, Yi Ting Chua,
12 Hong, W.C.H., Chi, C., Liu, J. et al. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Educ Inf Technol 28, 439–470 (2023). https://doi.org/10.1007/s10639-022-11121-5
13 Zwilling, M. et al. (2022) ‘Cyber Security Awareness, Knowledge and Behavior: A Comparative Study’, Journal of Computer Information Systems, 62(1), pp. 82–97. doi: 10.1080/08874417.2020.1712269.
14 M. Alanazi, M. Freeman, and H. Tootell, “Exploring the factors that influence the cybersecurity behaviors of young adults,” Computers in Human Behavior, vol. 128, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0747563222001984
15 Khan, N.F., Ikram, N., Saleem, S. et al. Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. Secur J 36, 373–405 (2022). https://doi.org/10.1057/s41284-022-00343-4
16 Debb, S. M., & McClellan, M. K. (2021). Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. Cyberpsychology, Behavior, and Social Networking, 24(9), 605-611.
17 A. Kovačević, N. Putnik and O. Tošković, "Factors Related to Cyber Security Behavior," in IEEE Access, vol. 8, pp. 125140-125148, 2020, doi: 10.1109/ACCESS.2020.3007867. keywords: {Computer crime;Internet;Information security;Cyberspace;Education;Password;Cyber security;cyber security behaviours;cyber security breaches;cyber security perception;knowledge;user awareness},
18 Isabel Arend, Asaf Shabtai, Tali Idan, Ruty Keinan, Yoella Bereby-Meyer, Passive- and not active-risk tendencies predict cyber security behavior, Computers & Security, Volume 97, 2020, 101964, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.101964.
19 A. Cuares and K. Casaña, “Digital responsibility of public administration students: Challenges and coping strategies,” Journal of Interdisciplinary Perspectives, vol. 4, no. 1, pp. 227–234, 2026. Available: https://doi.org/10.69569/jip.2025.744
20 R. Garcia et al., “The effects of exposure to online activities on cybersecurity awareness among rural internet users,” 2026.
21 J. D. P. Loyola, C. R. V. Batangan, C. J. A. Datu, J. A. Espiritu, R. R. G. Lim, and M. K. D. Cabaccan, "Age and Susceptibility: The Impact of Age on the Cyberattack Susceptibility of Parañaque Citizens," DLSU Senior High School Research Congress Conference Proceedings, vol. 5, no. 4, pp. 1–10, 2026. [Online]. Available: https://animorepository.dlsu.edu.ph/dlsushsresconproceedings/vol5/iss4/2/
22 M. Mahinay and J. Mamasalagat, “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, 2025.
23 D. Pasia, “Digital safety awareness and cybercrime prevention among community residents in the Philippines,” International Journal of Science and Advanced Technology, 2025. https://www.ijsat.org/papers/2025/4/8517.pdf
24 J. Diaz, “Assessing the relationship between young professionals’ perceptions of cybersecurity and their online shopping behaviour on e-commerce platforms in Koronadal City, Philippines,” 2025. https://www.researchgate.net/profile/Jayson-Diaz/publication/391512422
25 M. De Guzman and J. Rivera, “Digital literacy and cybersecurity behavior among Metro Manila residents,” 2024. https://doi.org/10.47895/amp.vi0.4894
26 B. L. Alabab et al., “Cybersecurity awareness of college students in a private higher education institution in the Philippines,” CGCI International Journal of Administration, Management, Education and Technology, vol. 1, no. 1, pp. 51–57, 2024.

27 J. U. Dapitan et al., "Measuring the level of cybersecurity awareness among senior high school students," Mediterranean Journal of Basic and Applied Sciences, vol. 8, no. 2, pp. 208–217, 2024. https://doi.org/10.46382/mjbas.2024.8216
28 N. B. B. Booc, K. Budiongan, and R. Carballo, "Cybersecurity awareness, perceived behavioral control, and cybersecurity behavior among high school students," EJASET, 2024.https://doi.org/10.59324/ejaset.2024.2(3).01
29 M. M. David and F. R. Odeste, "Fraud awareness and attitudes towards online banking: Perceived risk as mediator," Business Research Journal, vol. 9, no. 1, pp. 56–65, 2023. https://ejournals.ph/article.php?id=27426
30 C. H. S. Toso et al., "Cybercrime awareness among senior high school students," Mediterranean Journal of Basic and Applied Sciences, 2023. https://doi.org/10.46382/MJBAS.2023.7218
31 D. T. C. Escobar, "Cybersecurity knowledge and practices among university stakeholders in Cagayan State University," 2022. https://journalppw.com/index.php/jpsp/article/view/7383
32 E. Rotas and M. Cahapay, "Do students' threat knowledge influence protective behaviors? Evidence from remote learning," Journal of Pedagogical Sociology and Psychology, 2021. https://doi.org/10.33902/JPSP.2021167595