

Cybersecurity Practices and Facebook Hacking Exposure among Residents of Barangay Ipil, Ormoc City

Renor N. Apela 

Author Information:

Sto Niño College of Ormoc Inc., Ormoc City,
Leyte, Philippines

Correspondence:

apelarenor63@gmail.com

Article History:

Date Received: July 18, 2026

Date Revised: July 24, 2026

Date Accepted: August 28, 2026

Date Published: September 30, 2026

DOI: <https://doi.org/10.67903/ijroms0276>

Document ID: 2026IJROMS0276

Recommended Citation:

Apela, R. N. (2026). Cybersecurity practices and Facebook hacking exposure among residents of Barangay Ipil, Ormoc City. *International Journal of Research on Multidisciplinary Studies*, 1(8), 521-532. <https://doi.org/10.67903/ijroms.0276>

Abstract. This study determined the cybersecurity practices and exposure to Facebook hacking incidents among residents of Barangay Ipil, Ormoc City. Specifically, it described the respondents' profile in terms of age, sex, civil status, and educational attainment; assessed their self-reported cybersecurity practices in terms of account security practices, phishing and social engineering awareness, user awareness, online behavior, and privacy settings management; determined their self-reported level of exposure to Facebook hacking incidents; and examined the relationship between cybersecurity practices and Facebook hacking exposure. A descriptive-correlational research design was employed, with a structured questionnaire administered to 384 respondents selected from a population of 9,479 residents. Data on cybersecurity practices and Facebook hacking exposure were based on the respondents' self-reported responses and were analyzed using frequency, percentage, mean, standard deviation, and Pearson's r . Findings showed that the respondents were predominantly aged 21 years and above, single, and had attained at least college-level education. Overall, self-reported cybersecurity practices were rated high, with very high ratings for account security practices, phishing and social engineering awareness, user awareness, and privacy settings management, while online behavior was rated low. Self-reported exposure to Facebook hacking incidents was also rated high, particularly in terms of phishing attempts, suspicious login activities, and awareness of hacking incidents. A statistically significant moderate positive relationship was found between cybersecurity practices and Facebook hacking exposure ($r = .54$, $p < .001$), indicating that respondents who reported higher levels of cybersecurity practices also tended to report higher levels of exposure. This association should not be interpreted as evidence of causation or temporal direction. The study concludes that despite generally high self-reported cybersecurity practices, self-reported exposure to Facebook hacking incidents remains evident, highlighting the need for sustained cybersecurity education and stronger, more consistent safe online behaviors, particularly in relation to phishing prevention, account security, and privacy management.

Keywords: Cybersecurity Practices; Cyber Threats; Facebook Hacking; Online Security

Introduction

The rapid advancement of digital technology has transformed how individuals communicate, access information, conduct business, and engage in social activities, with Facebook becoming a widely used platform for communication, education, commerce, and social interaction. However, the widespread use of Facebook has also increased users' exposure to Facebook hacking, referring to unauthorized access or compromise of Facebook accounts that may result in the misuse of personal information, privacy, and online identity. Such exposure may occur through phishing, social engineering, suspicious login attempts, malicious links, weak account security practices, and other cyber threats. In this context, cybersecurity practices including account security, phishing and social engineering awareness, user awareness, safe online behavior, and privacy settings management play an important role in protecting Facebook accounts from unauthorized access. Thus, examining Cybersecurity Practices and Facebook Hacking Exposure is essential to understanding users' reported cybersecurity practices and their reported exposure to Facebook hacking incidents, and to providing a basis for strengthened cybersecurity education and preventive measures.

Moreover, cybercrime has emerged as a growing global concern accompanying the expansion of information and communication technologies. In Bangladesh, rapid technological advancement has accelerated digital transformation across communication, business, education, and governance while simultaneously contributing to the increasing incidence of cybercrime. With more than 130 million internet users as of 2023, the country has experienced a substantial rise in cyber offenses such as identity theft, online fraud, digital harassment, data breaches, and cyberextortion. Women and young people have been disproportionately affected, particularly through blackmail and harassment on social media platforms. Despite the enactment of the Digital Security Act of 2018 and the Cyber Security Act of 2023, institutional limitations and inadequate public awareness continue to hinder effective cybercrime prevention and enforcement (Rahman & Kaiser, 2025).

Similarly, cybercrime trends in Nepal demonstrate the increasing vulnerability of social media users. Dhital (2025) analyzed 53,474 cybercrime cases reported to the Nepal Police Cyber Bureau from fiscal years 2020/2021 to 2024/2025. The study found that reported cybercrime cases increased from 3,906 to 16,139 during the five-year period, peaking at 19,730 cases in 2023/2024. Facebook and Messenger accounted for approximately 72.73% of all reported cybercrime incidents, making them the primary platforms exploited by cybercriminals. Common offenses included hacking, unauthorized access, impersonation, online fraud, ransomware attacks, revenge pornography, photo manipulation, and defamation. These findings underscore the growing importance of strengthening cybersecurity awareness and promoting safe online behavior among social media users.

In the Philippines, the government has recognized the importance of information and communication technologies in national development and cybersecurity. Article XIV, Section 10 of the 1987 Philippine Constitution recognizes the vital role of science and technology in promoting national progress and improving the quality of life of the people. This constitutional mandate is reinforced through Republic Act No. 10844, or the Department of Information and Communications Technology (DICT) Act of 2015, which institutionalized the promotion and strategic use of information and communication technologies to improve governance, economic competitiveness, and public service delivery. Likewise, Republic Act No. 11293, or the Philippine Innovation Act, promotes innovation and technological advancement as drivers of sustainable national development.

Complementing these initiatives is Republic Act No. 10175, otherwise known as the Cybercrime Prevention Act of 2012, which provides the country's principal legal framework for combating cybercrime. The Act criminalizes offenses such as illegal access or hacking, illegal interception, data and system interference, computer-related fraud, identity theft, cybersquatting, cybersex, child pornography, unsolicited commercial communications, and online libel. The law likewise strengthens the government's capability to investigate, prosecute, and prevent cyber-related offenses while promoting cybersecurity awareness, responsible digital citizenship, and the protection of information systems.

Recent Philippine studies likewise emphasize the importance of public awareness and community participation in addressing cybercrime. Bueno (2026) evaluated the anti-cybercrime campaigns of the Quezon City Police District Anti-Cybercrime Team using a qualitative research design involving interviews, documentary analysis, immersion, and thematic analysis. The findings revealed that cybercrime victimization was associated with excessive social media use, limited digital literacy, misplaced trust in online information, age-related technological challenges, and economic vulnerability. The study further reported that awareness campaigns, community seminars, social media information drives, digital forensic support, volunteer participation, and inter-agency collaboration contributed to improved public awareness and confidence in reporting cybercrime. Moreover, official records indicated a nearly 34% reduction in cybercrime incidents following the implementation of these interventions, highlighting the value of sustained cybersecurity education and community engagement.

Although previous studies have documented the increasing prevalence of cybercrime and evaluated cybersecurity awareness in different national and institutional contexts, limited empirical evidence exists regarding the relationship between cybersecurity practices and Facebook hacking exposure at the community level in the Philippines. In particular, little is known about how residents' cybersecurity practices influence their exposure to Facebook hacking incidents in local communities such as Barangay Ipil, Ormoc City. Addressing this gap is essential for developing localized cybersecurity interventions and strengthening community-based digital safety programs.

Accordingly, this study aimed to determine the cybersecurity practices and Facebook hacking exposure among residents of Barangay Ipil, Ormoc City. Specifically, it described the respondents' demographic characteristics; assessed their cybersecurity practices in terms of account security practices, phishing and social engineering awareness, user awareness, online behavior, and privacy settings management; determined their level of exposure to Facebook hacking incidents; and examined the

relationship between cybersecurity practices and Facebook hacking exposure. The findings are expected to provide empirical evidence that can guide policymakers, local government units, educational institutions, law enforcement agencies, and community organizations in designing evidence-based cybersecurity awareness programs, strengthening digital safety initiatives, and promoting responsible online behavior among social media users.

Research Questions

This study aimed to determine the cybersecurity practices and Facebook hacking exposure among residents of Barangay Ipil, Ormoc City. Specifically, it sought to answer the following questions:

1. What is the demographic profile of the respondents in terms of:
 - 1.1 Age;
 - 1.2 Sex;
 - 1.3 Civil Status; and
 - 1.4 Educational Attainment?
2. What is the level of cybersecurity practices of the respondents in terms of:
 - 2.1 Account Security Practices;
 - 2.2 Phishing and Social Engineering Awareness;
 - 2.3 User Awareness;
 - 2.4 Online Behavior; and
 - 2.5 Privacy Settings?
3. What is the level of exposure of the respondents to Facebook hacking incidents?
4. Is there a significant relationship between the respondents' cybersecurity practices and their level of exposure to Facebook hacking incidents?

Scope and Delimitations of the Study

This study focused on determining the cybersecurity practices and Facebook hacking exposure among residents of Barangay Ipil, Ormoc City. It covered the respondents' demographic profile in terms of age, sex, civil status, and educational attainment. It also assessed their cybersecurity practices in terms of account security practices, phishing and social engineering awareness, user awareness, online behavior, and privacy settings. In addition, the study determined their level of exposure to Facebook hacking incidents and examined the significant relationship between cybersecurity practices and Facebook hacking exposure. The study was limited to the selected residents of Barangay Ipil, Ormoc City who participated as respondents. It focused only on the identified demographic characteristics, cybersecurity practices, and exposure to Facebook hacking incidents. Other social media platforms and cybersecurity issues not included in the research questions were beyond the scope of the study.

Literature Review

Okari *et al.* (2025) explored how the frequency of social media use influences exposure to cyber threats among Gen Z influencers, with particular emphasis on malicious link clicks, misinformation, and data breaches. Adopting a longitudinal design, the research monitored 100 Facebook influencer pages in Kisii County, Kenya, each with a minimum of 5,000 followers. Data were collected over a four-week period, yielding 440 observations. Collected information encompassed user demographics, platform engagement metrics (such as time spent online, number of posts, and login frequency), as well as security indicators including clicks on suspicious links, reports of misinformation, and breach incidents. Generalized Estimating Equations (GEE) were utilized to assess the influence of usage patterns on cybersecurity outcomes. Results indicated that interaction with suspicious links was the most significant predictor of data breaches, whereas extended time spent on Facebook correlated with a lower risk—likely reflecting increased platform familiarity and more cautious behavior. Other variables, such as posting frequency, content sharing, and follower growth, showed limited effect. To classify users by risk level, the study introduced a Security Threat Index (STI), revealing that individuals aged 18–20 were particularly vulnerable. Although the reliance on a convenience sample of young Facebook users constrains broader applicability, the research underscores the importance of extending studies to other platforms and age groups. The study helps identify high risk users and guide targeted interventions. Theoretically, the study advances Cybersecurity and Consumer Behavior theories by linking digital engagement patterns to cyber risk, contributing to the growing field of behavioral cybersecurity. It offers a new approach to quantifying cyber risk and improving digital safety among Gen Z influencers.

Hazarika (2025) reported the impact of cybersecurity breaches on undergraduate students' use of social media, with a specific focus on their awareness levels, experiences with cyber threats, and adoption of protective behaviors. Conducted as a case study at The Assam Royal Global University, India, the research utilizes a quantitative survey method involving 300 undergraduate participants across various disciplines. The findings reveal that while 72% of students claim awareness of online threats such as phishing, malware, and identity theft, only 25% have received any form of formal cybersecurity training. Notably, 38% of respondents reported having experienced at least one form of cyber-attack, with phishing being the most prevalent (50%), followed by unauthorized account access (20%) and malware infections (15%). The study further uncovers significant consequences of these breaches, including loss of privacy (44%), academic disruptions such as missed deadlines or lost assignments (26%), and heightened levels of anxiety and stress (65%) among affected students. Although some protective practices like adjusting privacy settings (70%) and using strong passwords (60%) are moderately adopted, more critical measures such as two-factor authentication (used by only 45%) and password managers (10%) remain underutilized. Furthermore, approximately 32% of students reported relying solely on basic password protection, leaving them highly vulnerable to attacks. The results underscore a critical gap between students' nominal awareness and practical cybersecurity preparedness. The study concludes that cybersecurity in higher education must be addressed not just as a technical issue, but as a matter of academic continuity and student mental health. It recommends that institutions integrate structured cybersecurity education, enforce policy-driven protective measures, and promote simulation-based awareness programs to build a more resilient student community in the digital age.

Talib (2025) believed that online social networks have become an inherent part of our lives today. These networks connect millions of people to their friends and family where they can share information using various social media platforms. Many people struggle to manage multimedia files such as audios, videos, and photos because of the inherent threat to privacy and confidentiality associated with these files. Therefore, any personal or sensitive information has the potential to go viral the moment it leaks out. Content that is leaked out can within minutes become a topic of discussion for people around the globe thanks to social networking platforms. The rise in social media use has ushered in a new era of online threats and attacks. Internet bullying, data theft, identity fraud, and phishing scams are just some of the risks that are threatening both individuals and organizations. The study analyses the social media impacts on cybersecurity and their negative consequences as well as measures that should be taken to mitigate the effects. Also, the study explained why proper User Awareness and Education is fundamental for ensuring cyber security.

Sharma and Jain (2025) also believed that with the emergence of technologies in the financial sector, various technologies are introduced in the sector. The prevailing technologies in the financial sector have forced organizations to adopt them to meet consumers' needs. The technologies are on the one hand making an operation flow very easy; but, on the other hand, it had invited many crimes also. According to the Reserve Bank of India, "Bank frauds of 100,000 and more have more than doubled in value to 1.85 lakh crores in the financial year 2020 as opposed to 71,500 crores in the financial year 2019." This digitalization era has given birth to cyberspace, and it has witnessed a larger cyberattack in Industry 4.0. To overcome these issues, some regulatory and legal frameworks are formed nationally and internationally. Their study outlines the overview of cybercrime, types of cyberattacks, challenges of cybersecurity, and prevention of cybercrime. In addition to it, the study also elaborates on the legal perspectives of cybercrime and their interpretations through various cases.

Kaufhold *et al.* (2025) conducted a study to determine the increasing vulnerability of citizens against cyberattacks, using the three representative surveys with German citizens in 2021 (N=1,093), 2023 (N=1,011), and 2024 (N=1,004) to examine their cyber threat awareness, use of protective security measures, and preferred information channels. While their findings attest large proportions of the German population a high level of cyber threat awareness, many citizens feel inadequately informed about coping with cyberattacks and show little confidence in German security authorities to protect citizens and infrastructures. While age correlated with citizens' awareness and behavior, they only saw minor temporal differences between datasets. Finally, they provide design and policy implications for enhancing citizens' awareness of cyber threats and implementing security measures.

Alshukri (2025) credited that social media networks have revolutionized global connectivity by enabling billions of users to engage in virtual communities and interact with one another; however, their widespread adoption has also attracted malicious actors who exploit platform vulnerabilities to compromise users' security and privacy. Despite the implementation of preventive measures, cyberattacks targeting social media platforms continue to increase, highlighting the need for advanced intrusion detection systems (IDS) and comprehensive security strategies. Although social media provides unprecedented convenience and

accessibility, many users lack the technical knowledge necessary to fully understand the privacy implications of the information they share, resulting in the ineffective use of available privacy and security settings. This study therefore proposes a holistic framework for social media security that integrates policy-driven safeguards and responsible user practices, including the use of strong passwords, regular credential updates, careful data sharing, reliable antivirus software, and legitimate and updated applications. Furthermore, Artificial Intelligence (AI) and Machine Learning (ML)-driven solutions can strengthen social media security through user sentiment analysis, disinformation detection, the prevention of illicit activities such as child trafficking, and adversarial machine learning techniques for enhancing intrusion detection systems. Ethical AI integration, consistent with the principles of "AI for Good," is also essential to minimize bias, promote fairness, and ensure responsible implementation of automated security mechanisms. Overall, the study examines recent developments in social media security and emphasizes the importance of protecting personal information amid increasing cyber threats and data breaches that may negatively affect economic stability and public trust. By integrating technological innovation, user awareness, ethical AI, and effective security policies, the proposed framework seeks to strengthen the trustworthiness, resilience, and security of social media platforms in an increasingly competitive and digitally connected world.

On the hand, Cornelius (2025) understood that despite the numerous advantages that smart cities offer, data security and privacy incidents can have serious consequences for citizens. Although South Africa is actively pursuing smart city initiatives, the surge in cyberattacks exacerbated by the heightened reliance on the Internet of Things (IoT) during the COVID-19 pandemic raises concerns regarding the security and privacy of citizens' data. The shift to smart cities also increases citizens' online presence, heightening the risk of cybercrime victimization. This article delves into the direct and indirect victims of data security and privacy incidents in emerging South African smart cities. Employing a quantitative research methodology, the article examines various facets, such as the identification of victims of data security and privacy breaches, their awareness of such incidents, instances of financial fraud, and the resulting financial losses experienced by victims. Drawing from data gathered through 317 web-based surveys conducted with South African citizens, the findings not only quantify the extent of victims affected but also shed light on the financial ramifications incurred by victims in emerging smart cities in South Africa. This paper lays the groundwork for addressing the critical need to protect both direct and indirect victims of data security and privacy incidents within the dynamic landscape of smart cities, thereby promoting the development of secure and resilient smart cities in South Africa and comparable international regions.

Methodology

Research Design

This study employed a quantitative research approach using a descriptive-correlational research design. The descriptive component was utilized to describe the respondents' demographic profile in terms of age, sex, civil status, and educational attainment, as well as to determine their level of cybersecurity practices in terms of account security practices, phishing and social engineering awareness, user awareness, online behavior, and privacy settings management. It also assessed the respondents' level of exposure to Facebook hacking incidents. The correlational component examined the relationship between the respondents' cybersecurity practices and their level of exposure to Facebook hacking incidents. This design was considered appropriate because it enabled the researcher to describe existing conditions and determine the statistical relationship between the independent variable, cybersecurity practices, and the dependent variable, Facebook hacking exposure, without manipulating either variable.

Sampling Design

The study employed simple random sampling. Using a 95% confidence level and a 5% margin of error, a sample size of 384 respondents was determined through a sample size calculator. After identifying residents who met the inclusion criteria, eligible respondents were assigned corresponding numbers, and the required number of participants was selected through a random-selection procedure, ensuring that each eligible resident had an equal probability of selection and helping minimize selection bias. The inclusion criteria required respondents to be residents of Barangay Ipil, maintain an active Facebook account, and voluntarily agree to participate in the study.

Research Locale

The study was conducted in Barangay Ipil, Ormoc City, Leyte, Philippines. The barangay was selected because of its large residential population and widespread use of social media platforms, particularly

Facebook, making it an appropriate setting for investigating cybersecurity practices and Facebook hacking exposure among community residents.

Research Participants

The research participants consisted of 384 eligible residents of Barangay Ipil, Ormoc City who were included in the study based on the established inclusion criteria. To qualify, respondents were required to be residents of Barangay Ipil, maintain an active Facebook account, and voluntarily agree to participate in the study. These criteria ensured that the selected participants met the requirements established for inclusion in the research.

Research Instrument

Data was collected using a structured questionnaire consisting of three parts. Part I gathered information on the respondents' demographic profile, including age, sex, civil status, and educational attainment. Part II measured cybersecurity practices in terms of account security practices, phishing and social engineering awareness, user awareness, online behavior, and privacy settings management. Part III assessed the respondents' exposure to Facebook hacking incidents. The questionnaire employed a five-point Likert scale, with higher scores indicating higher levels of cybersecurity practices or Facebook hacking exposure. For each scale, item responses were coded from the lowest to the highest response category, and the weighted mean was computed to determine the overall level of each construct. The corresponding verbal interpretations were based on the predetermined ranges of the five-point scale. The questionnaire was adapted from the studies of Shah and Agarwal (2020) and Wilsem (2013) and modified to align with the objectives, variables, and local context of the present study. Because the original instruments were adapted and modified, the resulting questionnaire was treated as an adapted instrument rather than an exact reproduction of the original scales. The Facebook hacking exposure measure was designed to capture a broad range of respondents' experiences and perceptions related to hacking incidents. Specifically, exposure included direct encounters with hacking incidents, indirect awareness of hacking incidents involving other people, and perceived prevalence or occurrence of Facebook hacking within the respondents' environment. This broader operationalization allowed the study to capture different ways through which respondents may encounter or become aware of Facebook hacking. However, this breadth also represents a measurement limitation, because the exposure score may combine actual personal experience with indirect awareness and perceptions of prevalence. Consequently, a higher exposure score should not necessarily be interpreted as evidence that the respondent personally experienced a hacking incident. The item concerning respondents' awareness of hacking strategies was interpreted cautiously. Although it contributes to the measurement of awareness related to Facebook hacking, responses to this item may also reflect the respondent's knowledge or familiarity with hacking strategies rather than actual exposure to a hacking incident. Thus, the item should not be interpreted independently as evidence of direct victimization or personal experience with hacking.

Data Gathering Procedure

Prior to data collection, permission to conduct the study was obtained from the Barangay Officials of Barangay Ipil, Ormoc City. After securing approval, the validated questionnaire was converted into an online survey using Google Forms. The researcher personally approached qualified respondents within the barangay and assisted them, when necessary, in accessing and completing the online questionnaire. Before participation, respondents were informed of the purpose of the study, the voluntary nature of their participation, and the confidentiality of their responses. Informed consent was obtained from all participants before data collection. Upon completion of the survey, responses were automatically recorded through Google Forms. The collected data were reviewed for completeness, and incomplete or invalid responses were excluded prior to statistical analysis.

Results and Discussions

Research Question 1: What is the demographic profile of the respondents in terms of: Age, Sex, Civil Status and Educational Attainment?

Table 1. Demographic Profile of the Respondents

Profile Variable	Category	Frequency (N)	Percentage (%)
Age	21 and above	265	69.01%
	19–20	54	14.06%
	17–18	34	8.85%
	15–16	31	8.07%
	Total	384	100%
Sex	Male	204	53.12%
	Female	170	44.27%
	Prefer not to say	10	2.60%
	Total	384	100%
Civil Status	Single	356	92.71%
	Married	26	6.77%
	Separated	2	0.52%
	Total	384	100%
Educational Attainment	College Level	171	44.53%
	College Graduate	85	22.14%
	Senior High School	76	19.79%
	Junior High School	52	13.54%
	Total	384	100.00%

The findings indicate that the respondents were predominantly young adults, male, single, and had attained at least a college-level education. These demographic characteristics suggest that the study largely captured individuals who are actively engaged in digital technologies and social media platforms, particularly Facebook, making them an appropriate population for examining cybersecurity practices and exposure to Facebook hacking incidents.

The predominance of respondents aged 21 years and above indicates that the study primarily involved individuals who are likely to have extensive experience using digital devices and online platforms. Young adults are generally more active internet users and rely heavily on social media for communication, education, entertainment, and commerce. Consequently, they are more likely to encounter cybersecurity risks, including phishing attacks, account compromise, identity theft, and other forms of cybercrime.

With respect to sex, the respondents were relatively balanced, although males slightly outnumbered females. This distribution suggests that cybersecurity practices and Facebook hacking exposure are relevant concerns for both men and women. The balanced representation also provides a broader perspective on cybersecurity behaviors across different groups of Facebook users.

The overwhelming majority of respondents were single, which may be associated with the relatively young age composition of the study population. Single individuals, particularly young adults, tend to spend more time on social networking platforms and online communication, increasing their opportunities for both beneficial online engagement and exposure to cyber threats. Their frequent use of Facebook and other digital platforms underscores the importance of promoting cybersecurity awareness and responsible online behavior among this demographic.

Regarding educational attainment, most respondents were either college-level students or college graduates. Higher educational attainment may contribute to greater digital literacy and increased awareness of cybersecurity risks, enabling individuals to recognize suspicious online activities and adopt safer online practices.

Overall, the demographic characteristics of the respondents provide an important context for interpreting the findings of the study. The predominance of young adults with relatively high educational attainment suggests that the respondents are active users of digital technologies and social media platforms, making them particularly relevant for investigating cybersecurity practices and Facebook hacking exposure. These characteristics also highlight the continuing need for cybersecurity education and awareness initiatives to encourage safe online behavior and reduce the risks associated with social media use.

Research Question 2: What is the level of cybersecurity practices of the respondents in terms of account security practices, phishing and social engineering awareness, user awareness, online behavior, and privacy settings?

Table 2. Level of Cybersecurity Practices among the Respondents (N-384)

Dimension	Mean	SD	Statistical Interpretation
Account Security Practices	4.34	0.68	Very High
Phishing and Social Engineering	4.30	0.65	Very High
User Awareness	4.36	0.65	Very High
Online Behavior	2.29	1.15	Low
Privacy Settings	4.24	0.71	Very High
Grand Mean	3.91	0.45	High

The findings indicate that the respondents demonstrated a high level of cybersecurity practices, with an overall mean of 3.91, suggesting that they generally employ measures to protect their online accounts, personal information, and digital activities from cybersecurity threats. Among the dimensions assessed, user awareness obtained the highest rating, followed by account security practices, phishing and social engineering awareness, and privacy settings management, all of which were interpreted as Very High. In contrast, online behavior received a Low rating, indicating that respondents do not consistently translate their cybersecurity knowledge into safe online practices.

The high ratings for user awareness, account security practices, phishing and social engineering awareness, and privacy settings management suggest that the respondents possess adequate knowledge of common cyber threats and recognize the importance of implementing preventive security measures. These findings imply that the respondents are generally capable of identifying cybersecurity risks and adopting protective practices such as using strong passwords, recognizing phishing attempts, and managing the privacy settings of their social media accounts.

However, the low rating for online behavior reveals an important behavioral gap. Although respondents appear knowledgeable about cybersecurity, they may not consistently apply this knowledge in their everyday online activities. This finding suggests that cybersecurity awareness alone does not necessarily lead to secure online behavior. Individuals may still engage in risky practices, such as clicking unknown links, using unsecured networks, or sharing personal information online, thereby increasing their vulnerability to cyber threats despite possessing adequate cybersecurity knowledge.

The present findings are consistent with the study of Shah and Agarwal (2020), who reported that individuals with higher levels of cybersecurity awareness generally demonstrate better security practices in protecting their digital accounts and personal information. Likewise, Bueno (2026) found that cybersecurity awareness campaigns and digital literacy initiatives improved public awareness and encouraged safer online practices among social media users. However, the low rating for online behavior supports the observations of Rahman and Kaiser (2025), who emphasized that cybercrime continues to increase despite growing public awareness because many internet users fail to consistently practice safe online behaviors. Similarly, Dhital (2025) identified Facebook as the primary platform associated with reported cybercrime incidents, highlighting the importance of consistently applying cybersecurity knowledge in everyday online activities.

Overall, the findings demonstrate that while the respondents possess a strong level of cybersecurity awareness and generally practice appropriate security measures, improving actual online behavior remains a significant challenge. This emphasizes the need for cybersecurity programs that not only increase users' knowledge but also promote the consistent adoption of safe online habits to reduce vulnerability to cyber threats and Facebook hacking incidents.

Research Question 3: What is the level of exposure of the respondents to Facebook hacking incidents?

Table 3. Level of Exposure to Facebook Hacking Incidents among the Respondents (N=384)

	Indicator	Mean	SD	Verbal Interpretation
1.	I have encountered phishing attempts on Facebook.	3.71	1.05	High
2.	I know someone who has experienced Facebook hacking.	3.88	1.09	High
3.	I have experienced suspicious login attempts.	3.92	0.99	High
4.	I am aware of common hacking strategies used online.	3.97	0.99	High
5.	Facebook hacking is common in my community or peer group.	3.84	1.03	High
	Grand Mean	3.87	0.84	High

The findings indicate that the respondents exhibited a high level of exposure to Facebook hacking incidents, as evidenced by the overall mean of 3.87 ($SD = 0.84$). This suggests that Facebook-related cyber threats are common among the respondents, either through direct personal experiences or indirect exposure within their social networks. The results imply that Facebook users remain vulnerable to various forms of cyberattacks despite increasing awareness of cybersecurity issues.

Among the indicators, respondents reported the highest level of agreement with the statement that they are aware of common hacking strategies used online, followed by experiences of suspicious login attempts. These findings suggest that the respondents are familiar with common cyber threats and have encountered activities that may indicate attempts to compromise their Facebook accounts. Such experiences reflect the growing sophistication and frequency of cyberattacks targeting social media users.

The respondents also reported knowing individuals who had experienced Facebook hacking and perceived Facebook hacking as common within their community or peer group. These findings indicate that exposure to Facebook hacking extends beyond individual experiences and has become a broader community concern. The widespread awareness of hacking incidents among peers may reflect the increasing prevalence of cybercrime and the rapid dissemination of information regarding online victimization through social networks. Although encountering phishing attempts on Facebook received the lowest mean among the indicators, it was still interpreted as High, suggesting that phishing remains a frequent threat encountered by the respondents. Because phishing is one of the most common methods used by cybercriminals to obtain unauthorized access to online accounts, its continued prevalence emphasizes the need for users to remain vigilant when interacting with links, messages, and online requests for personal information.

The present findings are consistent with those of Dhital (2025), who reported that Facebook and Messenger accounted for approximately 72.73% of reported cybercrime incidents in Nepal, identifying these platforms as the primary targets of cybercriminal activity. Likewise, Rahman and Kaiser (2025) observed that the rapid expansion of internet and social media use has been accompanied by increasing incidents of identity theft, online fraud, digital harassment, and other cyber offenses, particularly among active internet users. Similarly, Bueno (2026) found that Facebook hacking, phishing, identity theft, and online scams were among the most frequently reported cybercrime incidents in Quezon City, highlighting the continuing vulnerability of social media users despite ongoing public awareness campaigns. Overall, the findings demonstrate that exposure to Facebook hacking incidents remains prevalent among the respondents. This indicates that cyber threats continue to evolve alongside the increasing use of social media platforms. Although users may be aware of common hacking strategies, awareness alone does not eliminate the risk of cyber victimization. These findings underscore the importance of strengthening cybersecurity education, promoting responsible online behavior, and encouraging the consistent application of preventive security measures to reduce exposure to Facebook hacking and other forms of cybercrime.

Research Question 4: Is there a significant relationship between the respondents' cybersecurity practices and their level of exposure to Facebook hacking incidents?

Table 4. Relationship Between Cybersecurity Practices and Facebook Hacking Exposure (N=384)

Variables	r	95% CI	p-value	Decision	Interpretation
Cybersecurity Practices and Facebook Hacking Exposure	.54	.462, .610	< .001	Reject Ho	Significant moderate positive relationship

The

findings revealed a statistically significant moderate positive relationship between respondents' self-reported cybersecurity practices and their self-reported level of exposure to Facebook hacking incidents, $r = .54$, $p < .001$, $df = 382$, with a 95% confidence interval of $[.462, .610]$. The confidence interval indicates that the population correlation is estimated to lie between .462 and .610, and because the interval does not include zero, it provides further support for the statistical significance of the observed positive association. Thus, respondents who reported higher levels of cybersecurity practices also tended to report higher levels of exposure to Facebook hacking incidents. Accordingly, the null hypothesis stating that there is no significant relationship between cybersecurity practices and Facebook hacking exposure was rejected.

The positive association should not be interpreted to mean that stronger cybersecurity practices cause greater exposure to hacking incidents. Since both variables were measured through self-reported responses, the observed relationship may partly reflect differences in respondents' awareness, recognition, recall, and reporting of cyber threats. Respondents with stronger cybersecurity awareness and protective practices may be more likely to recognize and report phishing attempts, suspicious login activities, unauthorized access attempts, and other cyber threats. Conversely, previous experiences with or awareness of cyber threats may have encouraged respondents to adopt stronger cybersecurity practices. These possible explanations cannot be established as causal relationships because the study employed a cross-sectional correlational design and relied on self-reported measures.

An alternative analysis excluding the indicator "I am aware of common hacking strategies used online" could not be performed because the available data consisted only of summary statistics and did not include the individual respondent-level responses required to recalculate the correlation coefficient. Therefore, no alternative correlation coefficient was estimated, and the reported correlation of $r = .54$ remains the appropriate result based on the available data.

Overall, the findings establish a statistically significant moderate positive association between self-reported cybersecurity practices and self-reported exposure to Facebook hacking incidents. The results suggest that stronger protective practices may coexist with greater awareness and recognition of cyber threats rather than necessarily preventing exposure to them. Consequently, cybersecurity education should extend beyond promoting protective practices to strengthening consistent and safe online behavior, particularly in recognizing phishing attempts, securing accounts, managing privacy settings, and responding appropriately to suspicious online activities.

Ethical Considerations

The study adhered to established ethical principles in conducting research involving resident respondents of Barangay Ipil, Ormoc City, Leyte. Ethical clearance and permission to conduct the study were obtained from the Punong Barangay of Barangay Ipil, Ormoc City, Leyte prior to data collection. Informed consent was obtained from all respondents after they were clearly informed of the study's purpose, procedures, voluntary nature, potential risks, and their right to refuse participation or withdraw at any time without penalty. For respondents aged 15–17, the researcher obtained parental or legal guardian consent and the respondents' assent before their participation. The minors were provided with an age-appropriate explanation of the study and were informed that participation was voluntary and that they could decline or discontinue participation at any time. The researcher ensured that participation of minors proceeded only after the required consent and assent were secured. The privacy, anonymity, and confidentiality of all respondents were strictly protected. No passwords, account credentials, private messages, or other sensitive Facebook information were collected. Data were used solely for academic purposes, securely handled, and reported in a manner that prevented the identification of individual respondents. Measures were also taken to minimize possible discomfort or harm when respondents discussed their experiences with Facebook hacking. The researcher-maintained research integrity by accurately analyzing and reporting the findings and properly acknowledging all sources used in the study.

Conclusions

Based on the findings of the study, the respondents were predominantly 21 years old and above, single, and had attained at least a college-level education, indicating that most respondents had sufficient educational exposure to understand basic cybersecurity concepts, online risks, and protective measures; the respondents demonstrated a high level of cybersecurity practices in terms of user awareness, account security practices, phishing and social engineering awareness, and privacy settings, but their comparatively low level of online safety behavior indicated a gap between cybersecurity knowledge and its consistent application in actual online activities, suggesting that knowledge of cybersecurity practices does not necessarily correspond to consistently applying protective behaviors; the respondents also reported a high level of exposure to

Facebook hacking incidents, particularly phishing attempts, suspicious login activities, and awareness of hacking incidents within their community, indicating that respondents may experience or encounter cyber threats despite reporting relatively high levels of cybersecurity awareness and practices; moreover, a statistically significant moderate positive relationship was found between cybersecurity practices and exposure to Facebook hacking incidents ($r = .54, p < .001$), indicating that respondents who reported higher levels of cybersecurity practices also tended to report higher levels of exposure to Facebook hacking incidents, although the cross-sectional and self-report design does not permit determination of the direction of the relationship and does not establish that cybersecurity practices increased exposure or that exposure to hacking incidents led to stronger cybersecurity practices, as the relationship may reflect respondents' simultaneous experiences, awareness, and reporting of cybersecurity threats; overall, the study concludes that cybersecurity practices and exposure to Facebook hacking incidents are significantly associated, but the nature and direction of this relationship cannot be established from the present study, and the findings should therefore be interpreted as an observed association rather than a causal relationship, recognizing that the cross-sectional design captures cybersecurity practices and reported exposure at a particular point in time and that self-report measures may reflect differences in awareness, recognition, and reporting of cyber incidents, thereby emphasizing the importance of examining both cybersecurity practices and actual online experiences when assessing Facebook hacking exposure among residents of Barangay Ipil, Ormoc City, Leyte.

Recommendations

Based on the findings of the study, the Local Government Unit (LGU) of Barangay Ipil, Ormoc City, in coordination with the Department of Information and Communications Technology (DICT) and other concerned agencies, should conduct regular community-based cybersecurity activities, including phishing-awareness sessions, simulated phishing examples, Facebook account security demonstrations, and brief orientations on recognizing suspicious links, messages, login alerts, and fraudulent requests, with emphasis on practical steps that residents can immediately apply when using Facebook and other social media platforms; educational institutions and community learning centers should integrate practical cybersecurity education into seminars, extension programs, and relevant academic courses through hands-on guidance on multi-factor authentication (MFA), password-strength and password-management practices, privacy-setting walkthroughs, and exercises for identifying phishing and social engineering techniques, emphasizing consistent application of cybersecurity practices rather than awareness alone; residents of Barangay Ipil should consistently apply appropriate cybersecurity practices when using Facebook and other online platforms by using strong and unique passwords, enabling multi-factor authentication, regularly reviewing privacy and security settings, monitoring login activity, avoiding suspicious links and messages, and verifying unfamiliar requests before responding, while recognizing that such practices cannot guarantee complete protection from hacking incidents; the LGU, in partnership with appropriate government agencies and law enforcement authorities, should establish or strengthen accessible cybercrime reporting and assistance mechanisms by providing a simple reporting guide, designated contact points, and orientation on appropriate actions following a suspected Facebook hacking incident, including securing the account, changing compromised credentials, documenting suspicious activities, and reporting the incident to the appropriate authorities; and future researchers should replicate the study in other communities and settings to assess the consistency and generalizability of the findings, examine additional variables such as digital literacy, frequency of internet and social media use, cybersecurity knowledge, awareness of cybersecurity laws, and previous cybercrime victimization, and consider longitudinal or mixed-methods designs to better examine changes in cybersecurity practices and reported hacking exposure over time.

References

- Alshukri, Z. D. F. (2025). Security content used to protect data from social media. *Alkadhim Journal for Computer Science*, 3(2), 67–83. <https://doi.org/10.61710/kjcs.v3i2.110>
- Bueno, F. P. (2026). Impact of campaigns of the Quezon City Police District Anti-Cybercrime Team against scams and frauds. *International Journal of Sustainability and Advanced Integrated Research*, 2(2), 1756–1762. <https://doi.org/10.65339/ijairs.V2.I2.380>
- Cornelius, F. P. (2025). The nexus of cybercrime and data security in emerging South African smart cities. *Acta Criminologica: African Journal of Criminology & Victimology*, 38(3), 63–87.
- Dhital, H. (2025). The evolving landscape of cybercrime in Nepal: A multi-year analysis of platform-specific trends and victim demographics (2077–2082 B.S./2020–2025 A.D.). *Applied Data Science and Analysis*, 2025, 165–177. <https://doi.org/10.58496/ADSA/2025/014>

- Hazarika, H. J. (2025). Impact of cybersecurity breaches on social media: A case study on undergraduate students. *Alexandria: The Journal of National and International Library and Information Issues*. Advance online publication. <https://doi.org/10.1177/09557490251340833>
- Kaufhold, M.-A., Bäuml, J., Bajorski, M., & Reuter, C. (2025). Cyber threat awareness, protective measures and communication preferences in Germany: Implications from three representative surveys (2021–2024). In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (pp. 1–20). Association for Computing Machinery. <https://doi.org/10.1145/3706598.3713795>
- Okari, Y. M., Akuku, C., & Nyamau, R. N. (2025). Cybersecurity risk of frequent social media use among Gen Z influencers: A case study of university student Facebook users in Kisii University, Kenya. *Management*, 16(2), 1–13.
- Philippine Statistics Authority. (2021). *Highlights of the Philippine population: 2020 Census of Population and Housing (2020 CPH)*. <https://psa.gov.ph/content/highlights-philippine-population-2020-census-population-and-housing-2020-cph>
- Rahman, M. M., & Kaiser, M. S. (2025). Technological advancement and the rise of cybercrime in Bangladesh: Trends, challenges, and policy responses. In *The Palgrave handbook of global social problems* (pp. 1–23). Springer Nature Switzerland.
- Republic Act No. 10175. (2012). *Cybercrime Prevention Act of 2012*. Republic of the Philippines.
- Republic Act No. 10844. (2016). *Department of Information and Communications Technology Act of 2015*. Republic of the Philippines.
- Republic Act No. 11293. (2019). *Philippine Innovation Act*. Republic of the Philippines.
- Shah, P., & Agarwal, A. (2020). Cybersecurity behavior of smartphone users in India: An empirical analysis. *Information & Computer Security*, 28(2), 293–318.
- Sharma, J., & Jain, A. (2025). Cybersecurity and crime in Industry 4.0: An analysis of legal aspects of cybercrime. In *The techno-legal dynamics of cybercrimes in Industry 5.0* (pp. 19–42).
- Talib, S. A. (2025). Cybersecurity in social media. *Al-Rafidain Journal of Engineering Sciences*, 3(2), 132–140.
- Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29(4), 437–453