

## **Cybercrime Awareness and Digital Security in Rural Palawan, Philippines: Insights for Evidence-Based Local Governance**

**Edison C. Gabileo, Arneil S. Enario\*, and Randy Olano**

*College of Public Administration and Management, Western Philippines University, Aborlan, Palawan*

*\*Correspondence Author [arneil.enario@wpu.edu.ph](mailto:arneil.enario@wpu.edu.ph)*

### **ABSTRACT**

While digital technology offers vital opportunities, such as remote work and e-commerce, to isolated regions like southern Palawan, it also exposes residents to rising cybercrime, creating an urgent need for this study to inform and guide the local government's protective safety measures. This study assessed community awareness of cybercrime and helped the community secure itself from cyber threats. Using the descriptive method, convenience sampling via the Sloven formula was used to determine the participants in Aborlan, Palawan. The mean and T-test were used for data analysis. A validated questionnaire was administered. The findings show that respondents (176) have a mean age of 43.2 years, and that their income comes from small businesses they established in the barangay. Their demographic profile influences their perceptions of the community's safety needs and awareness of digital activities. The respondents believe that reporting cybercrime helps prevent future incidents, and sex significantly influences the measured variable, with females showing higher responses than males at the 0.05 level of significance. Based on respondents' suggestions, schools teach students digital citizenship and cybersecurity, emphasizing the importance of understanding digital footprints and applicable rules. The seminar aims to raise community awareness of cyber threats, such as hacking, phishing, and scams, to help detect suspicious online activity and, in case of an emergency, report to the proper authority, such as the Anti-Cybercrime Unit or the Philippine National Police. This study concluded that strengthening awareness of cybercrime in rural areas is important to address the increasing threats to the digital environment. This requires a comprehensive plan to raise community awareness and ensure that the LGU's municipal and provincial-wide initiatives develop policies and guidelines for awareness-raising and reporting when crimes occur. Those initiatives lessen the threats of cybercrime. This study recommends initiating a cybercrime awareness plan that includes studies of crime incidence, cyber best practices, cyber reporting, and implementation-related issues. The plan includes the adoption and formulation of policies from the local government units, the province, and the municipal government.

**Keywords:** Safe digital practices, information security, municipal policymaking, data-driven local governance, communication technology

### **INTRODUCTION**

Digital technology has empowered individuals and enterprises to engage in previously unattainable activities, such as remote work, online learning, and e-commerce, providing vital access to information and income opportunities (United Nations Office on Drugs and Crime 2023). This increased reliance on digital activities has opened new horizons for communication, commerce, and employment. People in remote areas, particularly in southern Palawan communities like Aborlan, are now being introduced to multimedia technologies previously accessible only in larger towns. As internet access expands in these southern regions, more residents are rapidly adopting social media, internet banking, and digital communication systems to connect more easily (Department of Information and Communication Technology 2023).

However, this rapid digital expansion exposes communities to severe risks, as Palawan remains highly vulnerable to cyber threats despite its geographic distance from more urbanized cities. Reports from the DICT (2023) and the Philippine National Police Anti-Cybercrime Group (PNP-ACG) (2022), emphasize a cumulative increase in cybercrime cases across the Philippines. This reliance on cyber activities has escalated threats like hacking and scamming, resulting in financial loss and severe psycho-emotional anguish for victims, especially women and young people (PNP-ACG 2022). Cybercrime further undermines public safety because structural resources or local prevention programs are often hard to find or unavailable in sufficient quantities.

To combat these threats, national frameworks such as the Cybercrime Prevention Act (RA 10175) and the Data Privacy Act (RA 10173) serve as vital legal instruments designed to protect, educate, and keep the public safe. Yet, for several reasons, regulatory protection and enforcement remain unequal across different parts of the country. Public safety is compromised when citizens lack awareness of these existing laws or the new mechanisms enacted to address digital offenses.

## **THEME: HEALTH, ENVIRONMENT, AND COMMUNITY WELL-BEING**

Recognizing these gaps, the province of Palawan and its Local Government Units (LGUs)—particularly at the barangay level—are actively implementing localized safety measures and enhancing digital security to protect residents in the province's southern region (Reynoso 2023). To address increasingly sophisticated global threats, contemporary cybersecurity frameworks emphasize international cooperation, risk assessment, and policy development (Laidlö and Jungbauer 2024; Lysenko et al. 2024), providing the standard protocols that local initiatives must align with to enhance cyber resilience (Craig et al. 2022).

This paper aims to assess the cybercrime awareness and digital security among selected barangays in the Municipality of Aborlan, Palawan, Philippines. As a descriptive baseline, the resulting empirical data and qualitative insights will directly serve as a foundational roadmap for local governance. By identifying critical vulnerabilities and institutional gaps at the grassroots level, this study will provide actionable recommendations to help barangay councils and the municipal government design localized cybersecurity policies, establish targeted digital literacy training programs, and deploy more effective community-level safety measures.

### **METHODS**

#### **Research Design**

This study utilized a descriptive research design. The researcher used convenience sampling, with the sample size determined by the Slovin formula; respondents were selected based on their accessibility and willingness to participate in the survey on cybercrime awareness.

#### **Research Respondents**

This study has 176 respondents, determined by the Slovin formula. These are the residents of the barangay Isaub, San Juan, and Jose Rizal, Aborlan, Palawan. These barangays were selected as they were the most network-accessible parts of the municipality, where they can access online technologies.

#### **Research Instruments**

This study utilized a survey questionnaire to collect data in the three rural barangays. The questionnaire was validated by IT practitioners and public administration professors through content validation.

#### **Data Treatment**

The scale was used to interpret the relationship between the respondents' scores and their corresponding levels of knowledge and agreement. Mean scores ranging from 4.21 to 5.00 were interpreted as Very High, indicating that respondents strongly agreed and demonstrated a strong level of awareness or practice. Scores ranging from 3.41 to 4.20 were interpreted as High, indicating that the majority of respondents agreed and were aware of the subject under study. Scores ranging from 2.61 to 3.40 were interpreted as Moderate, reflecting a neutral or moderately aware response. Scores ranging from 1.81 to 2.60 were interpreted as Low, indicating that respondents disagreed with or had limited knowledge of the topic. Finally, scores ranging from 1.00 to 1.80 were interpreted as Very Low, indicating that respondents strongly disagreed and exhibited minimal awareness or understanding. A *t*-test was used to determine the significant relationship between the identified common threats in digital security and the demographic profiles of respondents.

### **RESULTS**

#### **Sociodemographic Profile of the Respondents**

This study gathered demographic data to establish respondents' identities, allowing researchers to verify participants' perspectives on cybercrime awareness and Digital Security in Rural Palawan, Philippines. Thus, Table 1 shows that most respondents are female (128 or 73%), while males account for 27%. The largest age group is 41–50 years old (57 or 32.39%); this is followed by 31–40 years old (51 or 29%), 51 years and above (45 or 25%), and 30 years old and below (23 or 13.1%). Most respondents (169 or 96.02%) are self-employed or run their own businesses. A small portion (3.41%) works in government agencies, and only one respondent (0.57%) is employed in a private agency. At the time of the survey, the majority were self-employed in small businesses within their barangays.

**Table 1.** Sociodemographic Profile of the Respondents. Note: *n*=Sample population number of respondents.

| PROFILE OF THE RESPONDENTS | FREQUENCY     | PERCENTAGES |
|----------------------------|---------------|-------------|
|                            | <i>n</i> =176 | (%)         |
| <b>Sex</b>                 |               |             |
| Male                       | 48            | 27.00       |

## THEME: HEALTH, ENVIRONMENT, AND COMMUNITY WELL-BEING

|                              |     |       |
|------------------------------|-----|-------|
| Female                       | 128 | 73.00 |
| <b>Age</b>                   |     |       |
| 30 and below                 | 23  | 13.10 |
| 31–40                        | 51  | 29.00 |
| 41–50                        | 57  | 32.39 |
| <i>Mean – 43.2 years old</i> |     |       |
| 51 and above                 | 45  | 25.57 |
| <b>Income sources</b>        |     |       |
| Business–self–employed       | 169 | 96.02 |
| Private agency employee      | 1   | 0.57  |
| Government agency            | 6   | 3.41  |

### Awareness of Recognizing the Common Threats

Based on the survey data collected (Table 2) from 176 respondents ( $n = 176$ ), the evaluation of the community's Recognition of Common Threats yields an overall mean score of 3.65, corresponding to a descriptive rating of Agree. The most pronounced finding in this category is the deep collective concern about community safety, as evidenced by the statement "They believe cybercrime is a serious issue in our community," which captures the highest level of consensus, with a mean of 4.47 (Strongly Agree). This acute awareness of local vulnerability is paired with a solid understanding of specific, severe offenses, as shown by the high agreement levels for the dangers of Online Sexual Exploitation of Children (OSEC) at 4.00 (Agree) and familiarity with the severe impacts of identity theft at 3.77 (Agree).

**Table 2.** Recognition of common threats in and their responses in Aborlan, Palawan from 176 respondents ( $n=176$ ).

| Recognition of Common Threats                                                          | (n=176)     |                |
|----------------------------------------------------------------------------------------|-------------|----------------|
|                                                                                        | Mean        | DR             |
| They are aware of common cyber threats, including scams, phishing, and fake job offers | 3.00        | Moderate Agree |
| They identified suspicious links or websites that may lead to hacking or malware.      | 3.00        | Moderate Agree |
| They understand the dangers of online sexual exploitation of children (OSEC).          | 4.00        | Agree          |
| They are familiar with cases of identity theft and their impact on victims.            | 3.77        | Agree          |
| They believe cybercrime is a serious issue in our community.                           | 4.47        | Strongly Agree |
| <b>Overall Mean</b>                                                                    | <b>3.65</b> | <b>Agree</b>   |

### Significant Findings on the Recognition of Common Threats in Terms of Sex

A comparative statistical analysis between male and female groups across specific metrics yielded a statistically significant result (Table 3). The female group had a higher mean score (4.04) than the male group (3.52), indicating a descriptive difference in their performance or responses. To determine if this difference was statistically meaningful, a hypothesis test was conducted. The analysis revealed a remarkably strong positive correlation coefficient ( $R = 0.9485$ ), suggesting a highly tight alignment in the data structure between the groups. With a calculated  $p$ -value of 0.0068, which falls well below the standard alpha significance level (0.05), the findings are highly significant. Because the test statistic surpassed the critical threshold ( $t$ -critical = 2.13), the null hypothesis is formally rejected. This confirms that the observed variation between the male and female variables is not due to random chance but represents a statistically significant difference.

**Table 3.** Significant findings on the recognition of common threats in terms of sex of the respondents (*T-TEST Level of Significance = 0.05*).

| Variables | Mean | R      | p-value | t-critical | Interpretation              |
|-----------|------|--------|---------|------------|-----------------------------|
| Male      | 3.52 | 0.9485 | 0.0068  | 2.13       | Reject the null hypothesis. |
| Female    | 4.04 |        |         |            |                             |

### Safe Digital Practices

The Safe Digital Practices of the 176 respondents ( $n = 176$ ), as shown in Table 4, yield a positive overall mean score of 3.80, indicating a descriptive rating of Agree. This indicates that the community generally

## THEME: HEALTH, ENVIRONMENT, AND COMMUNITY WELL-BEING

implements proactive measures to secure its digital footprint. Among the assessed behaviors, the respondents demonstrated the highest commitment to personal data privacy, strongly agreeing with the practice of avoiding oversharing personal information online, with a mean score of 4.28 (Strongly Agree). This strong protective instinct toward personal information is supported by strong compliance with credential management and privacy controls, as evidenced by high agreement with using strong, unique passwords (4.03, Agree) and with reviewing and adjusting social media privacy settings (3.74, Agree).

**Table 4.** Safe digital practices related to cybercrime and security measures among respondents of Aborlan, Palawan (n=176).

| Safe Digital Practices                                                    | n=176       |                |
|---------------------------------------------------------------------------|-------------|----------------|
|                                                                           | Mean        | DR             |
| Regularly update my devices and software to protect against cyberattacks. | 3.29        | Moderate Agree |
| Use strong and unique passwords for my online accounts.                   | 4.03        | Agree          |
| Review and adjust my social media privacy settings.                       | 3.74        | Agree          |
| Avoid oversharing personal information online                             | 4.28        | Strongly Agree |
| Only download applications and files from trusted sources.                | 3.68        | Agree          |
| <b>OVERALL MEAN</b>                                                       | <b>3.80</b> | <b>Agree</b>   |

### Reporting and Support Mechanisms among Respondents

Table 5 presents survey data on reporting and support mechanisms among the 176 respondents (n = 176), indicating a highly favorable outlook, with all indicators reflecting consensus or strong agreement. The most notable finding is the community's profound belief in civic duty and collective security, as evidenced by the statement "They believe reporting cybercrime helps prevent future incidents," which secured an overwhelming mean score of 4.81 (Strongly Agree). This reflects an exceptional level of proactive intent and awareness regarding the value of crime documentation. This high ideological support translates well into general practical knowledge, as respondents agreed they know where to report if they or someone they know becomes a victim of cybercrime (mean of 3.89), which is backed by a solid foundation of institutional confidence, seen in their trust that law enforcement agencies will act against reported cases (3.69) and their personal confidence in reporting cybercrime cases to authorities (3.63).

**Table 5.** Reporting and support mechanisms of respondents in terms of cybercrime and security measures in Aborlan, Palawan (n=176).

| REPORTING AND SUPPORT MECHANISMS                                                    | n=176 |                |
|-------------------------------------------------------------------------------------|-------|----------------|
|                                                                                     | Mean  | DR             |
| They know where to report if I or someone I know becomes a victim of cybercrime.    | 3.89  | Agree          |
| They feel confident in reporting cybercrime cases to authorities.                   | 3.63  | Agree          |
| They trust that law enforcement agencies will act against reported cybercrime cases | 3.69  | Agree          |
| They are aware of hotlines or online platforms for reporting cybercrime.            | 3.48  | Agree          |
| They believe reporting cybercrime helps prevent future incidents.                   | 4.81  | Strongly Agree |

### Gaps and Challenges in Cybercrime

The survey data in Table 6, collected from a sample of 176 respondents (n = 176), indicate that evaluating institutional gaps and community challenges highlights critical areas of concern, with all listed items receiving agreement or strong agreement, as observed in Table 4. The most severe challenge identified by the respondents is the Insufficient Local Cybercrime Prevention Programs, which garnered the highest mean score of 4.65 (Strongly Agree). This is closely followed by Weak Institutional and Policy Frameworks at the LGU Level, with a mean score of 4.50 (Strongly Agree), emphasizing a significant demand for stronger local governance and localized cybersecurity initiatives.

**Table 6.** Gaps and challenges on cybercrime and security measures in Aborlan, Palawan (n=176).

| GAPS AND CHALLENGES                                      | n=176 |                |
|----------------------------------------------------------|-------|----------------|
|                                                          | Mean  | DR             |
| Lack of Community Awareness and Digital Literacy         | 4.00  | Agree          |
| Insufficient Local Cybercrime Prevention Programs        | 4.65  | Strongly Agree |
| Limited Knowledge of Legal Rights and Reporting Channels | 4.00  | Agree          |

## **THEME: HEALTH, ENVIRONMENT, AND COMMUNITY WELL-BEING**

|                                                           |      |                |
|-----------------------------------------------------------|------|----------------|
| Weak Institutional and Policy Frameworks at the LGU Level | 4.50 | Strongly Agree |
| Rapid Technological Changes and Emerging Threats          | 3.79 | Agree          |

### **DISCUSSION**

#### **Sociodemographic Profile of the Respondents**

In rural Philippine municipalities like Aborlan, traditional primary industries such as farming and fishing often draw men away from the household during the day, leaving women to anchor local community life through household management, community associations, and neighborhood microenterprises. Consequently, cybercrime awareness campaigns, such as community extension seminars and information literacy drives, must be intentionally tailored to engage this highly active female population. Because mothers and female community leaders serve as the primary managers of household information in these rural setups, educating them creates a powerful, localized trickle-down effect that effectively safeguards children and the elderly from online threats (Taufik et al. 2022).

This age profile signals a noteworthy digital literacy gap. Individuals aged 31 and older are generally "digital immigrants" who did not grow up with smartphones or the internet. Digital immigrants, particularly older adults, have adopted smartphones and other digital technologies later in life, often driven by necessity in professional environments (Thangavel and Chandra 2024). They are statistically more vulnerable to social engineering tactics, such as phishing, smishing (SMS scams mimicking banks or government lotteries), and online misinformation. Because their baseline familiarity with evolving cybersecurity threats is lower than that of the younger generation, digital security training in Aborlan must avoid overly technical jargon and focus on practical, step-by-step protective behaviors.

Most respondents are self-employed or run small businesses in their barangays, while a small fraction work in government or private agencies. In a rural economy like Aborlan's, formal corporate infrastructure is limited. Local livelihoods depend heavily on independent micro-, small-, and medium-sized enterprises (MSMEs), agricultural trade, and informal neighborhood commerce (Daulay 2025).

#### **Awareness of Recognizing the Common Threats**

The respondents have a generally strong collective baseline awareness of digital safety risks in the locality. The community possesses a strong emotional and conceptual firewall, but a weak technical defense. Residents deeply fear the consequences of cybercrime but are only moderately equipped to recognize the entry points (e.g., clicking a compromised link) that enable it, as cited by Cross et al. (2021). The study reports that a majority of community members view cybercrime as a serious problem in Australia, a finding also observed in the Philippines. The Federal Trade Commission (2023) explains that suspicious links and fake websites are commonly used to deliver malware or steal personal information, resulting in low awareness among residents.

#### **Significant Findings on the Recognition of Common Threats in Terms of Sex**

Female respondents registered a significantly higher mean score than male respondents. This indicates that women in this sample are more aligned with safe digital practices, have higher legal literacy, and exhibit a more acute recognition of cyber threats than their male counterparts. The exceptionally high Pearson correlation coefficient indicates that, although the absolute scores differ (women consistently score higher), the patterns of their responses are almost perfectly synchronized. If males scored an item low (e.g., technical software updates), females also scored it relatively lower; if females scored an item exceptionally high (e.g., community concern over OSEC or data privacy), males did too. They share the same perceptual priorities, but women maintain a consistently higher baseline of agreement or vigilance. The correlation shows that men and women share the same structural strengths and vulnerabilities. Therefore, educators and internal auditors designing community extension programs do not need to build separate educational materials for each gender. The content of the cybersecurity modules (focusing heavily on technical threat detection and reporting platforms) can remain the same; only the delivery and outreach strategies need to be customized to ensure that both genders are reached effectively. Increasing gender diversity in cybersecurity not only addresses representation but also enhances team effectiveness and innovation, as diverse perspectives contribute to more comprehensive solutions (Pacheco 2024).

#### **Safe Digital Practices**

A respondent can have an incredibly strong password and share nothing on social media, yet remain highly vulnerable if they are running an outdated operating system. Cybercriminals frequently exploit unpatched system vulnerabilities to execute malware or spyware behind the scenes. This means a user's device could still be compromised without them ever revealing their password or oversharing data. Because the majority of respondents are self-employed or run small businesses in their barangays (Table 1), their smartphones serve as both business tools and digital wallets (e.g., GCash, Maya). Running outdated operating systems exposes these

## **THEME: HEALTH, ENVIRONMENT, AND COMMUNITY WELL-BEING**

critical financial lifelines to device-level exploits, turning a simple software neglect into a severe financial risk that could compromise their working capital. Auxier et al. (2019) state that most Americans are concerned about how their personal information is used online and take steps to limit what they share. The result aligns with the Philippines' awareness. At the same time, the CISA (2023) explains that regularly updating software and devices is one of the most effective ways to protect against cyberattacks and known vulnerabilities, which contrasts with the results of this study.

### **Reporting and Support Mechanisms Awareness among Respondents**

The highest score in this dataset is for the belief that reporting cybercrime helps prevent future incidents. This indicates that the community does not view reporting as merely a reactive or punitive measure to recover lost funds; rather, they see it as a proactive, preventative tool for community safety. In close-knit rural barangays, security and peace of mind are collective responsibilities. This exceptional score suggests that respondents possess a strong sense of solidarity—they are highly motivated to report a crime if it means protecting their neighbors, relatives, and fellow business owners from falling into the same trap. While the willingness to report is exceptionally high, the lowest relative score in this framework is for actual awareness of specific digital hotlines and online platforms. This creates a subtle operational bottleneck. The community is mentally and emotionally prepared to cooperate with the law, but they lack immediate, friction-free access to the exact technical tools needed to initiate that contact. Conversely, while technology can enhance community-police relations, it may also introduce new challenges, such as surveillance concerns and the potential for exacerbating existing mistrust, particularly in marginalized communities (Törn 2023).

### **Gaps and Challenges in Cybercrime**

The primary reason for these high scores is that while cybersecurity is managed at a macro level by national agencies (such as the PNP-ACG or the National Privacy Commission), these frameworks rarely trickle down effectively to rural, municipality-level governance. Local Government Units (LGUs) in developing areas often lack the technical expertise, budget, and localized ordinances required to enforce digital safety. Because the majority of the respondents in this demographic are self-employed or run small businesses within their barangays, they rely heavily on digital platforms and mobile wallets (e.g., GCash) to survive. When they encounter digital threats, they realize there are no local municipal desks, emergency hotlines, or localized counseling programs to support them. This lack of a nearby safety net drives the intense consensus that local programs are insufficient. To address these critical governance gaps, the Aborlan Local Government Unit (LGU) must swiftly enact localized municipal ordinances that mandate cybersecurity budgets, formalize operational data privacy protocols, and establish a dedicated digital complaints desk. To overcome the resource constraints of building an independent IT security framework, the LGU should strategically collaborate with local academic institutions. By leveraging university community extension services to deliver targeted information literacy initiatives, the municipality can efficiently transform the academic sector into the proactive grassroots prevention program the community urgently demands. Latifiyah (2025) mentioned that targeted drives can address specific literacy gaps, such as digital and financial literacy, which are crucial for community empowerment and informed decision-making.

### **Respondents' Suggestions for improvement**

Based on the responses to the open-ended questions, the respondents recommended that individuals take responsibility for their own computer safety, with parents providing guidance to children on internet privacy, safety, and online etiquette. They further suggested that schools teach students digital citizenship and cybersecurity, emphasizing the importance of understanding digital footprints and adhering to applicable rules. In addition, the respondents recommended that community seminars be conducted to raise awareness of common cyber threats, such as identity theft and scams. These suggestions align with Internet Safety Basic Rules and Recommendation (ISBRR) (2025), which notes that digital security involves parental guidance on internet privacy and safety, complemented by school instruction on digital citizenship and cybersecurity, underscoring the importance of understanding digital footprints and practicing responsible online behavior.

### **FUNDING**

With in-kind support of Western Philippines University.

### **GENERATIVE AI STATEMENT**

The concepts, results, and discussion within this paper are the authors' original work and represent their independent contribution. AI tools, specifically Grammarly (version 1.2.210.1786) and Gemini 2.5 Pro, were used solely for manuscript editing, grammar refinement, and readability improvement. These tools were not involved in data generation, analysis, interpretation of results, or the formulation of primary arguments.

### **DECLARATION OF COMPETING INTEREST**

The authors declare no competing interests.

## ACKNOWLEDGMENTS

The author thanks the College of Public Administration and Management and their superiors for their support. The author also thanks the experts who evaluated the methodology and the respondents' output, as well as the editors, statisticians, and reviewers who helped improve the manuscript.

## REFERENCES

- Auxier B, Rainie L, Anderson M, Harrison A, Rodgers M. 2019. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Pew Research Center. <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>
- Craig A, Johnson RAJ, Gallop M. 2022. Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies. *Journal of Cyber Policy*. 7(3):375–396. <https://doi.org/10.1080/23738871.2023.2178318>
- Cross C, Holt T, Powell A, Wilson M. 2021. Responding to Cybercrime: results of a Comparison Between Community Members and Police Personnel. Canberra (AU): Australian Institute of Criminology.
- CISA (Cybersecurity and Infrastructure Security Agency). 2023. Secure our world: Simple ways to protect yourself, your family, and your business online. U.S. Department of Homeland Security. <https://www.cisa.gov/secure-our-world>
- Daulay SM. 2025. Potret UMKM Desa Pantai Labu: analisis tantangan, strategi dan kontribusi ekonomi lokal. *Smart Goals: jurnal Bisnis Digital dan Manajemen*. 1(2):61–80. <https://doi.org/10.36490/jsg.v1i2.1863>
- DICT (Department of Information and Communications Technology). 2023. National Cybersecurity Plan 2023–2028. Government of the Philippines.
- FTC (Federal Trade Commission). 2023. How to recognize and avoid phishing scams [Internet]. Washington (DC): Federal Trade Commission; [accessed 2026 May 20]. Available from: <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
- ISBRR (Internet Safety Basic Rules and Recommendations). 2025 [Internet]. [accessed 2026 May 20]. <https://doi.org/10.5281/zenodo.17204783>
- Laidlő C, Jungbauer C. 2024. Cybersecurity policy framework: requirements for establishing highly interoperable and interconnected health data spaces. *Frontiers in Medicine*. 11. <https://doi.org/10.3389/fmed.2024.1379882>
- Latifiyah F. 2025. Pengabdian masyarakat merupakan upaya peningkatan literasi dan kesejahteraan. *Masyarakat Mandiri*. 2(2):32–43. <https://doi.org/10.62951/masyarakatmandiri.v2i2.2102>
- Lysenko S, Liubchenko A, Kozakov V, Demianchuk Y, Krutko Y. 2024. Global cybersecurity: harmonizing international standards and cooperation. *Multidisciplinary Reviews*. 7. <https://doi.org/10.31893/multirev.2024spe021>
- Pacheco F. 2024. Gender diversity in cybersecurity: gaps, challenges, and proposals. In: 2024 IEEE Region 10 Conference (TENCON). <https://doi.org/10.1109/TENCON62399.2024.10735942>
- PNP–ACG (Philippine National Police Anti–Cybercrime Group). 2022. Annual cybercrime statistics and public safety awareness report. Camp Crame, Quezon City: PNP–ACG.
- Reynoso I. 2023. DICT trains Palawan LGUs on digital connectivity techniques. Philippine News Agency. <https://www.pna.gov.ph/articles/1205592>
- RA 10173 (Republic Act No. 10173). 2012. An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes. Official Gazette of the Republic of the Philippines. <https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/>
- RA 10175 (Republic Act No. 10175). 2012. An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties therefor and for Other Purposes. Official Gazette of the Republic of the Philippines. <https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/>
- Taufik CM, Subaer S, Lusiawati L, Suminar E, Ghassan R, Sila GE, Hasarudin D, Adiya K, Turyono J, Bintang G, et al. 2022. Literasi untuk menumbuhkan kesadaran tentang media sosial bagi ibu rumah tangga. *Jurnal Abdimas Sang Buana*. 3(2):61–68. <https://doi.org/10.32897/abdimaasangbuana.v3i2.1735>
- Thangavel P, Chandra B. 2024. Digital immigrants versus digital natives: decoding their e-commerce adoption behavior. *SAGE Open*. 14(4). <https://doi.org/10.1177/21582440241282437>
- Törn C. 2023. Surveilled subjects and technologically mediated law enforcement. In: cambridge University Press eBooks. 304–322. <https://doi.org/10.1017/9781108924304.016>
- UNODC (United Nations Office on Drugs and Crime). 2023. Digital citizenship education handbook. Paris (FR): UNESCO Publishing.

**ROLE OF AUTHORS:** ECG – conceptualization, data gathering, and instrument validation of the manuscript; ASE – analysis, language editing, citation and referencing and revising the manuscript.

### Suggested citation:

Gabileo EC, Enario AS, Olano R. 2026. Cybercrime Awareness and Digital Security in Rural Palawan, Philippines: Insights for Evidence–Based Local Governance. In: Dolorosa RG, Trestiza KAJ, Mabuhay-Omar JA, Diamante JT, Mecha JPF, Gimarangan JA and Espartero SAM (Eds.), *RIDE Annual Conference Proceedings* (Vol. 1, pp. 79–85). Western Philippines University, Palawan, Philippines.