

Assessing Awareness of Predatory Mobile Lending Applications Among Residents of Tolosa, Leyte

Ma. Joan Piedad Advincula

Debbie Karylle F. Arquero, College of Criminal Justice Education, University of the Cordilleras, Baguio City, Philippines

Abstract

This study examined the level of awareness of predatory mobile lending applications among residents of Tolosa, Leyte, a municipality in Eastern Visayas where poverty incidence remains high. Mobile lending apps have rapidly expanded across the Philippines, offering convenience but also exposing users to exploitative practices such as excessive interest rates, harassment, and privacy violations. Using a quantitative approach, structured surveys were administered to 393 respondents. Results revealed that while mobile lending apps are widely recognized, awareness of predatory lending risks remains critically low, with 85.5% of respondents reporting insufficient understanding of these risks. These findings highlight significant knowledge gaps in financial literacy and underscore the need for targeted educational interventions to protect vulnerable populations.

Keywords: cyber fraud, financial literacy, legal remedies, mobile lending applications

INTRODUCTION

Cybercrime has evolved alongside the growth of computing and internet technologies, encompassing both technical attacks and social engineering schemes (Alghamdi, 2020; Schmitt & Flechais, 2023). Globally, the cost of cybercrime reached \$8.44 trillion in 2022 and is projected to rise to \$23.84 trillion by 2027 if conditions remain unchanged (Charlton, 2024). Social engineering, which manipulates human psychology rather than exploiting technical vulnerabilities, has become a dominant method of victimization, costing organizations more than \$100,000 on average per incident and taking longer to contain (Sjouwerman, 2023; Sjouwerman, 2024).

In the Philippines, cybercrime has surged in tandem with widespread internet and smartphone use. As of January 2024, there were 86.98 million internet users, representing a penetration rate of 73.6% of the population, with young adults disproportionately represented online (Kemp, 2024). Filipinos spend an average of 5 hours and 47 minutes daily on smartphones, including 3 hours and 34 minutes on social media (Howe, 2024; Kumar, 2025). This heavy online presence has contributed to rising cybercrime, with the Philippine National Police Anti-Cybercrime Group reporting a 94.64% increase in online scams between 2022 and 2023 (Argosino, 2024).

Predatory mobile lending apps represent a particularly harmful form of cyber-enabled fraud. These apps promise quick access to small loans but often impose exorbitant interest rates, hidden fees, and aggressive collection practices. In Kenya, rates can reach 20% (Munyendo et al., 2022), while in India they range from 25% to 75% per annum (Saritha, 2023). Locally, reports indicate harassment of borrowers and extraction of contact information from their devices (personal communication, February 14, 2024). Victims have suffered severe psychological consequences, including depression and suicide (Aggarwal et al., 2024).

Tolosa, Leyte, situated in Region VIII Eastern Visayas, is particularly vulnerable due to high poverty incidence – 22.7% in Leyte province and 26.1% in the region overall (Mapa, 2024). Economic hardship drives residents toward quick-access financial solutions, making them susceptible to predatory lending. This study focused on assessing the level of awareness of predatory mobile lending apps among Tolosa residents, providing localized insights into financial literacy gaps and consumer vulnerability.

METHODOLOGY

This study employed a quantitative research design to assess the level of awareness of predatory mobile lending applications among residents of Tolosa, Leyte. A structured survey questionnaire served as the primary data-gathering tool. The instrument was designed to capture respondents' recognition of mobile lending apps and their understanding of the risks associated with predatory practices, including excessive interest rates, hidden fees, harassment, and privacy violations.

A total of 393 residents of Tolosa participated in the study. Respondents were selected purposively to ensure inclusion of individuals who had access to mobile lending apps or had encountered them in their community. The sample size was sufficient to provide a reliable snapshot of awareness levels across different demographic groups, although the present article focuses only on overall awareness rather than demographic differences.

The survey questionnaire was structured to elicit both recognition of mobile lending apps and awareness of predatory features. Items were designed to measure respondents' self-reported knowledge of risks such as high interest rates, aggressive collection practices, and privacy violations. The instrument was administered in person, and responses were recorded systematically.

Data collection was conducted with the cooperation of local residents who consented to participate. To ensure accuracy, responses were checked for completeness before inclusion in the dataset. The survey results were then compiled and subjected to descriptive statistical analysis.

The data were analyzed using descriptive statistics to determine the proportion of respondents who demonstrated sufficient awareness of predatory lending risks. Percentages were calculated to reflect the overall distribution of awareness levels. In addition, the raw counts of respondents were reported to provide clarity on the extent of knowledge gaps.

Ethical standards were observed throughout the study. Informed consent was obtained from all participants, and personal identifiers were excluded from the dataset to protect confidentiality. Sensitive information, such as names and contact details, was not recorded, ensuring that the privacy of respondents was maintained.

RESULTS

The survey of the residents of Tolosa, Leyte revealed that mobile lending applications are widely recognized in the community. However, awareness of predatory lending risks remains critically low. Out of the total respondents, 85.5% reported insufficient understanding of predatory practices, while only 14.5% demonstrated moderate to high awareness of exploitative features such as excessive interest rates, hidden fees, and harassment.

This indicates that while recognition of mobile lending apps is nearly universal among respondents, the majority lack substantive knowledge of the risks. The data confirmed that knowledge gaps in financial literacy persist across the community, leaving a significant portion of the population vulnerable to exploitation.

These results underscore a troubling disconnect between recognition of mobile lending apps and awareness of their predatory features. In Tolosa, Leyte, residents may be drawn to the convenience of these platforms without fully understanding the risks. This finding aligns with broader studies that emphasize the dangers of digital lending in low-income contexts, where financial desperation often overrides caution (Munyendo et al., 2022; Saritha, 2023).

The high percentage of respondents reporting insufficient awareness highlights the urgent need for targeted financial literacy programs. Community-based education campaigns, particularly those delivered through accessible channels such as schools and social media, could help bridge these knowledge gaps. Without such interventions, residents remain at risk of falling into cycles of debt and harassment perpetuated by predatory mobile lending practices.

Comparative evidence reinforces the severity of the issue. In India and Kenya, predatory lending apps have imposed crippling interest rates and fees, leading to widespread victimization (Munyendo et al., 2022; Saritha, 2023). In the Philippines, regulatory bodies such as the Securities and Exchange Commission and Bangko Sentral ng Pilipinas have attempted to curb abusive practices through legislation, including the Lending Company Regulation Act of 2007 and the Truth in Lending Act. However, enforcement challenges persist, and many victims remain unaware of their rights or distrustful of authorities.

The psychological toll of predatory lending is also significant. Victims have reported anxiety, depression, and feelings of vulnerability (Jansen & Leukfeldt, 2018; Palassis et al., 2021). In extreme cases, harassment by lending apps has led to suicide (Aggarwal et al., 2024). These findings highlight that awareness is not merely a matter of financial literacy but also of mental health and community resilience.

CONCLUSION AND RECOMMENDATIONS

The findings of this study demonstrate that while mobile lending applications are widely recognized among residents of Tolosa, Leyte, awareness of their predatory features remains critically low. Out of the 393 respondents surveyed, 85.5% admitted to insufficient understanding of the risks associated with these apps, leaving only 14.5% with moderate to high awareness of exploitative practices such as excessive interest rates, hidden fees, harassment, and privacy violations. This knowledge gap exposes a significant portion of the community – 336 individuals out of the total sample – to potential financial exploitation. These results highlight that financial literacy in Tolosa is inadequate to protect residents from predatory lending practices. Although familiarity with mobile lending apps is nearly universal, the lack of awareness regarding their dangers reinforces cycles of vulnerability. Poverty and limited access to traditional financial institutions exacerbate this problem, making quick-access digital loans appealing despite their harmful consequences. The data confirmed that socio-economic conditions play a decisive role in shaping awareness, with lower-income groups particularly at risk of exploitation.

Based on the findings of this study, several recommendations are put forward. First, financial literacy initiatives must be strengthened in schools and communities to increase awareness of predatory lending risks. Educational campaigns should be regulated and disseminated through accessible platforms, including social media, to combat misinformation and improve consumer decision-making. Second, accessibility to legal remedies must be enhanced by establishing legal aid programs and public awareness campaigns that specifically target victims of predatory lending. Such measures would encourage residents to seek justice and reduce the stigma associated with reporting exploitation. Finally, financial knowledge gaps among lower-income groups must be bridged through free and inclusive education programs, ensuring that all residents, regardless of socio-economic status, have equal access to consumer protection resources.

Together, these recommendations emphasize the urgent need for targeted interventions that address both financial literacy and legal empowerment. By implementing these measures, the community of Tolosa, Leyte can be better equipped to resist predatory mobile lending practices and safeguard its residents against cycles of financial vulnerability.

REFERENCES:

1. Aggarwal, V., Aggarwal, N., Dhingra, B., Batra, S., & Yadav, M. (2024). Predatory loan mobile apps in India: a new form of cyber psychological manipulation. *ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems*. <https://doi.org/10.1109/icetis61505.2024.10459589>
2. Alghamdi, M. I. (2020). A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide. *International Journal of Engineering Research And*, 9(6). <https://www.ijert.org/research/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide-IJERTV9IS060565.pdf>
3. Argosino, F. (2024, July 1). Cybercrimes up by 21% in 1st quarter, says PNP. *INQUIRER.net*. <https://newsinfo.inquirer.net/1956595/cybercrimes-up-by-21-in-1st-quarter-says-pnp>
4. Charlton, E. (2024). 2023 was a big year for cybercrime – Here's how we can make our systems safer. In *World Economic Forum*. World Economic Forum. <https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/>
5. Howe, S. (2024, May 6). Social media statistics in the Philippines [Updated 2024]. *Meltwater*. <https://www.meltwater.com/en/blog/social-media-statistics-philippines>
6. Jansen, J., & Leukfeldt, R. (2018). Coping with Cybercrime Victimization: An Exploratory Study into Impact and Change. *Journal of Qualitative Criminal Justice and Criminology*, 6(2). <https://cybersciencecenter.nl/media/1258/jansen-leukfeldt-2018-coping-with-cybercrime-victimization.pdf>
7. Kemp, S. (2024, February 20). *Digital 2024: The Philippines – DataReportal – Global Digital Insights*. DataReportal – Global Digital Insights. <https://datareportal.com/reports/digital-2024-philippines>
8. Kumar, N. (2025, April 7). *Smartphone Usage Statistics 2025 (Worldwide Data)*. DemandSage. <https://www.demandsage.com/smartphone-usage-statistics/>
9. Mapa, C. D. S. (2024). Percentage of Filipino families classified as poor declined to 10.9 percent in 2023. In *Philippine Statistics Authority* (No. 2024-232). Republic of the Philippines, Philippine Statistics Authority. <https://www.psa.gov.ph/system/files/phdsd/Preliminary%202023%201st%20sem%20Poverty%20Statistics%20Tables.xlsx>
10. Munyendo, C. W., Acar, Y., & Aviv, A. J. (2022). "Desperate Times Call for Desperate Measures": User Concerns with Mobile Loan Apps in Kenya. *2022 IEEE Symposium on Security and Privacy (SP)*. <https://doi.org/10.1109/sp46214.2022.9833779>
11. Palassis, A., Speelman, C. P., & Pooley, J. A. (2021). An exploration of the psychological impact of hacking victimization. *SAGE Open*, 11(4), 215824402110615. <https://doi.org/10.1177/21582440211061556>
12. Saritha, M. (2023). Demystifying the misery behind loan apps in India. *Indian Journal of Finance and Banking*, 104-109. <https://doi.org/10.46281/ijfb.v13i1.2047>
13. Schmitt, M., & Flechais, I. (2023). Digital Deception: Generative artificial intelligence in social engineering and phishing. *arXiv (Cornell University)*. <https://doi.org/10.48550/arxiv.2310.13715>

14. Sjouwerman, S. (2023, August 23). Data Breaches Involving Social Engineering Attacks Take Longer to Identify and Contain. *Security Awareness Training Blog*. <https://blog.knowbe4.com/data-breaches-social-engineering-attacks>
15. Sjouwerman, S. (2024, November 11). [Eye opener] Attackers don't hack, they log in. Can you stop them? *Security Awareness Training Blog*. <https://blog.knowbe4.com/eye-opener-attackers-dont-hack-they-log-in.-can-you-stop-them>
16. Varga, G. (2022, May 27). Global Cybercrime Report: Which Countries Are Most at Risk?. SEON. Retrieved September 17, 2022, from <https://seon.io/resources/global-cybercrime-report/>
17. Zulkiffli, S. N. H., Zawawi, M. N. A., & Rahim, F. A. (2020). Passive and active Reconnaissance: a Social Engineering case study. *2020 8th International Conference on Information Technology and Multimedia*, 138–143. <https://doi.org/10.1109/icimu49871.2020.9243402>