

Truth, Trust, And Trickery: Older Adults' Experiences With Misinformation And Scams In Cabuyao, Laguna

¹Jhonson A. Rebosura

²Edward Francis G. Gabor

¹ Pamantasan ng Cabuyao

¹ jhonsonrebosura2005@gmail.com

¹ <https://orcid.org/0009-0000-6278-1082>

² Pamantasan ng Cabuyao

gaboredwardfrancis@gmail.com

DOI: <https://doi.org/10.63084/cognexus.v2i2.308>

Abstract

The rapid advancement of digital technologies has increased the vulnerability of older adults to misinformation and fraud, posing potential threats to their financial security, privacy, trust, and psychological well-being. The current study investigated the experiences of older adults aged 45–65 living in the City of Cabuyao, Province of Laguna, who encountered various scams or misinformation. Theoretical models that guided this study include Media Literacy Theory and the Digital Information Disorder Framework, and the method employed in the research was a qualitative phenomenological design. Participants of the study included four older adults aged 45–65 who lived in the City of Cabuyao and used digital services. Purposive and snowball sampling were used to select the participants. Semi-structured interviews were conducted with the participants, and a phenomenologically oriented thematic analysis was used to analyze the information obtained. Inductive analysis generated four themes in the study: (1) navigating digital risks and fraudulent threats; (2) credibility assessment shaped by familiarity and verification practices; (3) emotional distress and reflective learning from scam encounters; and (4) protective strategies and social support in scam avoidance. The participants identified impersonation, requests for sensitive information, fraudulent transactions, and deceptive online services. The findings showed that participants' assessments of credibility were influenced by familiarity and perceived legitimacy. Scam encounters also elicited various emotional responses and encouraged participants to become more vigilant in evaluating information and protecting themselves from potential fraud.

Keywords: older adults; misinformation; fraud; digital literacy; digital fraud; credibility assessment; scam awareness

Introduction

Digital technologies have become increasingly integrated into everyday communication, information seeking, financial transactions, and social interaction. In addition to their advantages, digital environments have facilitated the rapid spread of misleading information and the emergence of fraud of different complexity levels. Manipulated multimedia content, imposters, false messages, fraudulent services, and requests for confidential information appear to be difficult to assess since they imitate people known to their receivers or trusted entities (University of Nevada, Reno, 2023; GSMA, 2025).

Studies associate media and digital literacy with the capability to check the veracity of information presented. Those who possess higher levels of media literacy are more willing to check the information before accepting it as true (Cai et al., 2024). However, older adults do face additional challenges caused by their limited experience in using computer technologies (Moore & Hancock, 2022). It is particularly relevant for the Philippines, where certain older adults possess limited ICT skills and are vulnerable to growing scams online (GSMA, 2025).

Previous studies have examined susceptibility to misinformation and fraud, credibility assessment, and prevention strategies among older adults. However, limited qualitative evidence describes how older adults experience, interpret, and respond to misinformation and scams within specific Philippine community contexts. In particular, little is documented about how older adults in Cabuyao, Laguna, assess credibility, experience the emotional consequences of scam encounters, and draw on family and community support when responding to digital risks. Addressing this contextual gap, the present study explores the lived experiences of older adults with misinformation and scams in Cabuyao. A qualitative local account provides insight into how credibility, emotional responses, protective practices, and social support are experienced within participants' everyday community and digital contexts, dimensions that may not be fully captured through broader survey-based or population-level studies. The primary research question is: What are the experiences of older adults regarding misinformation and scams in the City of Cabuyao?

Literature Review and Theoretical Framework

Misinformation, scams, and vulnerability

Vulnerability to misinformation and scams does not necessarily imply susceptibility to fraud. Cognitive, social, behavioral, and economic factors determine how victims react to fake

information (Anspach & Carlson, 2022; DeLiema et al., 2025). For instance, scam companies manipulate many different communication channels to play upon people's everyday online habits and beliefs while knowing that potential victims are neither trained to verify dubious content nor facilitate crime reporting (Houtti et al., 2024; Joseph et al., 2022). Such risks may be aggravated by the social gaps due to unfamiliar technologies, social isolation, and financial difficulties that older adults often face while falling victims to one or another scam technique (Beach et al., 2020; Parti et al., 2025).

Credibility, trust, and digital literacy

The evaluations of credibility processing in social media contexts depend on previous contacts with the source, the user's perceptions of the source, and the media patterns that the user was exposed to (Cha, 2024). Older adults might use familiar people, recognizable institutions, professional websites, testimonials, and reviews as signs of credibility. While these signs may help to identify legitimate information, they can also be misused. Thus, digital and media literacy serves as an important level of protection, which helps to evaluate the source, question it, and verify its information (Bada, 2025; Burau Grain & Cedeño Moreira, 2026; Rasi et al., 2021).

Emotional impact and protective support

The consequences of fraud may extend beyond monetary loss. For instance, fear, anxiety, humiliation, trauma, and loss of confidence may arise (Button et al., 2025). Interestingly, older adults benefit from experience as they develop ways of protecting themselves and learn how to check on information sources, examine comments, be wary of inappropriate messages, and confirm information with other people (Bailey et al., 2020; Baines & Hargittai, 2025).

Theoretical framework

The foundation of the study was built upon Media Literacy Theory (Potter, 2004) and the Digital Information Disorder Framework (Wardle & Derakhshan, 2017). Media Literacy Theory brings to light how people can utilize knowledge and skills to judge media content as well as to value source credibility. The Digital Information Disorder Framework serves to categorize various types of misleading information and how it spreads within digital environments. Together, these frameworks guided the examination of how participants encountered fraudulent or misleading content, assessed credibility, and responded to scam attempts.

Methodology

Research design and setting

The study employed a qualitative phenomenological design to examine the meanings participants attached to their lived experiences with misinformation and scams. Phenomenological inquiry was appropriate because the study sought detailed descriptions of how participants encountered, interpreted, and responded to misinformation and scams and the meanings they derived from these experiences (Englander & Morley, 2021; Moustakas, 1994). The study was conducted in Cabuyao, Laguna, an urbanized component city where digital platforms are widely used for communication and transactions.

Participants and Sampling

The final analytic sample consisted of four participants, as confirmed by the available interview records containing complete responses for Participants 1–4. Participants were selected based on the eligibility criteria established in the original study protocol. To be included, participants had to be 45–65 years old, residents of Cabuyao, Laguna, regular users of a smartphone, tablet, or comparable digital device, and users of at least one digital platform, such as Facebook, Messenger, TikTok, X (formerly Twitter), text messaging, or phone calls. Participants must also have experienced or encountered misinformation or a scam attempt, whether online or offline and whether or not the attempt resulted in successful deception or financial loss. Individuals who did not meet the specified age, residency, digital-device use, digital-platform use, or misinformation/scam-experience criteria were excluded from the study. Purposive sampling was initially used to identify individuals who met these criteria, followed by snowball sampling through participant referrals.

The 45-year lower threshold was established in the original study protocol to capture experiences associated with the transition and ageing process rather than to equate the study population with the legal category of senior citizens. This age criterion is supported by Perianayagam et al. (2022), whose Longitudinal Ageing Study in India (LASI) included adults aged 45 years and older to examine ageing-related transitions that may begin before conventional old age. Accordingly, the term “older adults” is retained as the original study terminology and is operationally defined in this study as participants aged 45–65 years. This

operational definition is specific to the present study and should not be interpreted as a legal classification of senior citizens.

The available study records did not document the exact recruitment period, a formal saturation-based stopping criterion, the specific basis on which recruitment was concluded, or additional individual demographic characteristics; therefore, these details could not be reconstructed or reported retrospectively.

Data collection

The data were gathered through semi-structured interviews, which were designed by the researcher. The interview questions focused on participants' experiences with misinformation and scams, their assessments of credibility, their emotional responses, and the strategies they used to evaluate information and prevent or respond to fraudulent activity. Because of the open-ended format of the interview, the participants were able to express themselves freely, and probing questions were utilized for clarity. Depending on the availability of the participants, the interviews were done personally or online.

Data analysis

The interview transcripts were analyzed using a phenomenologically oriented thematic process informed by Moustakas (1994) and supported by the qualitative analytic approach discussed by Gabor and Montillano (2025). The primary researcher conducted the initial analysis by reading the transcripts multiple times to become familiar with the participants' accounts and to maintain attention to their descriptions of the phenomenon. Significant statements directly reflecting participants' encounters with misinformation and scams, credibility assessments, emotional responses, and protective practices were identified and examined for their underlying meanings.

The significant statements were organized into related meaning units, which were subsequently grouped into categories based on recurring patterns across the participants' accounts. From these categories, broader themes were inductively developed. The co-author and research mentor reviewed the developing categories, themes, and interpretations in relation to the interview data. The analysis was revisited when necessary to ensure that the resulting themes remained coherent and grounded in participants' accounts. This review served to strengthen the interpretive consistency of the analysis rather than constitute independent coding or a

formal intercoder reliability procedure. The use of recurring themes as a basis for qualitative interpretation was further supported by Gabor and Montillano (2025).

Throughout the analysis, the primary researcher practiced reflexivity by remaining conscious of how prior knowledge and assumptions about digital misinformation, vulnerability, and scam experiences could influence interpretation. Interpretations were continually checked against participants' significant statements and verbatim accounts. Although the analysis was informed by phenomenological principles, it did not employ the complete sequence of Moustakas' transcendental phenomenological procedures, such as formal epoché, separate textural and structural descriptions, and a composite synthesis of the essence. Accordingly, the analytic procedure is reported as a phenomenologically oriented thematic analysis rather than as a complete Moustakas-style transcendental phenomenological analysis.

Ethical considerations

The study underwent ethical review by the Research Ethics Review Committee prior to data collection, under the oversight of Dr. Maria Emmalyn Asuncion D. Capuno, Chair of the Research Ethics Review Committee. Participants were informed in writing about the study's purpose, procedures, potential risks and benefits, voluntary nature of participation, and their right to withdraw without penalty. Written informed consent was obtained from all participants, including explicit permission to audio-record the interviews. Participants were also allowed to decline to answer questions, pause the interview, or discontinue their participation if they experienced discomfort while discussing misinformation or scam-related experiences.

To protect confidentiality, participant names and other direct identifiers were excluded from the reported data, and participant codes were used in the transcripts and presentation of findings. Audio recordings, transcripts, and other electronic research materials were stored in password-protected digital storage accessible only to the primary researcher. The data were used solely for academic research purposes and were handled in accordance with the Data Privacy Act of 2012 (Republic Act No. 10173).

Results

Inductive analysis of the four participant interviews produced four themes corresponding to the study's areas of inquiry. The synthesis table summarizes the themes and subordinate patterns. The narrative below presents anonymized verbatim excerpts from Participants 1–4 so that the

interpretations can be traced directly to the interview data. Literature-based comparison is reserved primarily for the Discussion.

Overarching theme	Key subordinate themes	Synthesis of findings
Navigating Digital Risks and Fraudulent Threats	Low scam awareness; identity fraud and trust exploitation; data exploitation and privacy breach; financial fraud and transaction deception	Participants described fraudulent calls, impersonation of relatives or agencies, requests for OTPs and phone access, and deceptive online transactions or services.
Credibility Assessment Shaped by Familiarity and Verification Practices	Reliance on familiarity; impersonation exploitation; surface-level verification; response to warning signs and intervention	Familiar identities, recognized institutions, professional-looking websites, testimonials, and reviews initially increased credibility; unusual requests and trusted third-party advice prompted reassessment.
Emotional Distress and Reflective Learning from Scam Encounters	Fear and anxiety; embarrassment and shame; betrayal and anger; reflective learning	Scam encounters caused emotional distress and concern for others, but participants also described learning to evaluate information more carefully.
Protective Strategies and Social Support in Scam Avoidance	Immediate defensive action; personal vigilance; family guidance; community support	Participants ignored suspicious messages, ended calls, double-checked information, delayed transactions, sought in-person verification, and consulted children, friends, or trusted peers.

Theme 1: Navigating digital risks and fraudulent threats

Participants encountered scams through phone calls, social media, online services, and digital transactions. Initial cooperation often occurred when the contact appeared to come from a familiar person or recognizable institution. Impersonation was especially salient when scammers claimed to represent a public agency or a relative. Requests for OTPs, phone access,

or other personal details created risks of account compromise, while other incidents involved paid services that became inaccessible or purchases for which the seller disappeared after payment.

Across the accounts, deceptive contact was not limited to one platform or one type of loss. Participants described compromised social-media accounts, attempted access to GCash, failed online services, and a seller who blocked a buyer after payment. These accounts show how routine digital interactions can become settings for privacy, identity, and financial risks.

Participant 3 described a paid online course: “I could access the first and second lessons, but when it came to the third lesson, I could no longer access it... I could no longer reach [the agent].”

Theme 2: Credibility assessment shaped by familiarity and verification practices

Participants initially assessed credibility through familiar identities and recognizable signs of legitimacy. Messages that appeared to come from relatives were easier to trust, while professional-looking websites, testimonials, videos, and positive reviews also served as credibility cues. These cues, however, could be imitated or manipulated.

Participant 1 explained: “I thought it was legitimate because Ate Mila was the first one who messaged me. I believed it was really her.”

Participant 4 said: “When I purchase an account, I first check the reviews... I look for any negative feedback or bad reviews to determine whether the seller is trustworthy.”

Credibility judgments changed when warning signs emerged, including repeated requests for OTPs, shifts in the conversation, account-access problems, or warnings from trusted people. Participants’ accounts therefore show a movement from familiarity-based trust toward more deliberate verification after suspicious cues appeared.

Theme 3: Emotional distress and reflective learning from scam encounters

Participants described fear, nervousness, embarrassment, betrayal, anger, and frustration after realizing that they had been deceived or that their accounts had been compromised. Distress was intensified when scammers used a participant’s identity to solicit money from others or when another person lost money because of the compromised account.

Participant 2 stated: “I was scared... someone still became a victim because of my account... One of my relatives sent money because... they genuinely thought I was the one asking for help.”

Participant 3 reflected: “I felt so betrayed. I was very angry... It taught me to be more critical, analytical, and cautious.”

Participants also interpreted the incidents as learning experiences. They described becoming more cautious about offers, requests for information, reviews, and online payments, and emphasized the need to verify before acting.

Theme 4: Protective strategies and social support in scam avoidance

Participants described immediate and preventive responses to suspected scams, including ending calls, ignoring suspicious messages, directly rejecting suspected scammers, double-checking information, delaying or avoiding transfers, and preferring in-person confirmation when feasible.

Participant 1 said: “If someone asks for links, codes, or similar information, I no longer give them out because of what happened to me before.”

Participant 3 explained: “I no longer transfer money online without thoroughly verifying everything first.”

Protection was also social. Children reminded participants not to disclose OTPs, helped secure financial accounts, and advised them about suspicious communications. Friends and people nearby shared warnings, intervened during suspicious calls, and helped validate questionable offers.

Participant 2 noted: “My children help me by constantly reminding me... Do not click links or open anything that strangers send you.”

Participant 4 added: “I also seek validation from friends to confirm whether the information or offer is legitimate before proceeding.”

Throughout the analysis, the primary researcher practiced reflexivity by continually checking interpretations against the participants’ statements and interview transcripts. Themes were developed inductively from recurring meaning units rather than predetermined by the theoretical framework. The co-author and research mentor reviewed the emerging themes and

interpretations to ensure their coherence and grounding in the data. This review served as an interpretive check rather than independent coding or formal intercoder reliability.

Discussion

The findings address the research question by showing that participants' experiences with misinformation and scams involved interconnected processes of encountering deceptive content, assessing credibility, experiencing emotional consequences, and developing protective responses. Across these experiences, credibility judgments were shaped by familiarity and perceived legitimacy, while subsequent warning signs, prior experiences, and social support encouraged more deliberate verification. Viewed through Media Literacy Theory and the Digital Information Disorder Framework, these accounts illustrate how participants navigated misleading or fraudulent information within everyday digital and interpersonal contexts. These interpretations are specific to the four participants and are intended to explain their experiences rather than establish causal relationships or population-level patterns.

The findings suggest that participants' initial responses to misinformation and scams were shaped partly by trust in familiar sources and recognizable signs of legitimacy. Participants did not simply accept messages because of limited knowledge; rather, deceptive communications often appeared to come from familiar individuals, recognized institutions, or seemingly legitimate online transactions. Initial credibility judgments therefore tended to change when participants encountered warning signs or inconsistencies. This finding can be understood through Media Literacy Theory, which emphasizes active evaluation of sources, purposes, and messages rather than reliance on surface-level indicators of credibility (Potter, 2004).

The findings also illustrate how information disorder operates within everyday digital interactions. Misleading messages and fraudulent information appeared across familiar communication channels, including social media, phone calls, text messages, and online services, making it difficult for participants to distinguish interpersonal trust from information credibility. Participants' experiences suggest that the social context in which a message is received may influence how its credibility is initially assessed. This finding is consistent with previous research linking social familiarity and source perceptions with credibility judgments (Cha, 2024).

The participants' experiences with privacy breaches, account-security risks, GCash-related incidents, failed online services, and fraudulent online transactions are consistent with previous research showing that routine risky behaviors, limited awareness of scam strategies, and

seemingly legitimate online interactions may contribute to fraud vulnerability (DeLiema et al., 2025; Houtti et al., 2024).

Another important finding concerns the emotional impact of scam encounters. Participants described fear, shame, betrayal, and anger in connection with financial loss, account breaches, and identity misuse. These experiences are consistent with previous research showing that the consequences of fraud may extend beyond financial harm and affect psychological well-being (Button et al., 2025). At the same time, participants described learning from these experiences by becoming more cautious and deliberate in verifying information before responding or taking action.

Finally, the findings indicate that participants relied on both individual protective practices and social support when responding to suspected scams. Participants described double-checking information, delaying transactions, and seeking confirmation before taking action. They also relied on children, friends, and members of their community for advice and verification. These findings suggest that interventions may combine practical digital literacy skills with family- and community-based verification strategies rather than focusing solely on individual technical knowledge.

Conclusion and Recommendations

Among the four older adults aged 45–65 in this Cabuyao study, misinformation and scams were experienced through fraudulent calls, impersonation, privacy and account-security breaches, deceptive online services, and fraudulent transactions. Familiar identities, institutional cues, professional-looking information, testimonials, and reviews shaped initial credibility judgments, while unusual requests and trusted third-party warnings prompted reassessment. Participants also described substantial emotional reactions and subsequent efforts to verify information more carefully. These findings are context-specific and are intended to illuminate lived experience rather than establish causal relationships or generalize to all older adults in Cabuyao, Laguna, or the Philippines.

Based on these accounts, community-based initiatives may emphasize practical verification skills, recognition of impersonation and OTP-related scams, protection of personal data, and safer payment practices. Family members and community networks may also be incorporated as verification supports when suspicious messages or transactions arise. Future studies should recruit more diverse participants, clearly document recruitment periods and stopping criteria,

and examine how experiences vary across age groups, communities, and levels of digital literacy.

Limitations

The study relied on selected participants' self-reported experiences in the City of Cabuyao, Province of Laguna. The findings are intended to provide an in-depth account of lived experience rather than statistical generalization to all older adults in Laguna or the Philippines. Experiences may also reflect the specific platforms, scam types, and social contexts encountered by participants at the time of data collection.

References

- Anspach, N. M., & Carlson, T. N. (2022). Not who you think? Exposure and vulnerability to misinformation. *New Media & Society*, 26(8), 4847–4866. <https://doi.org/10.1177/14614448221130422>
- Bada, K. (2025). Digital literacy and information disorder: Understanding older adults' interaction with false information on social media. *Path of Science*. <https://pathofscience.org/index.php/ps/article/view/3706>
- Bailey, J., Taylor, L., Kingston, P., & Watts, G. E. (2020). Older adults and 'scams': Evidence from the Mass Observation Archive. *The Journal of Adult Protection*, 23(1), 57–69. <https://doi.org/10.1108/JAP-05-2020-0018>
- Baines, A., & Hargittai, E. (2025). Older adults' responses to misinformation on social media. *AoIR Selected Papers of Internet Research*. <https://spir.aoir.org/ojs/index.php/spir/article/view/13901>
- Beach, S., Czaja, S. J., et al. (2020). Vulnerability to financial scams among older adults: Cognitive and psychosocial factors. *Innovation in Aging*, 4(Suppl. 1), 447. <https://doi.org/10.1093/geroni/igaa057.1458>
- Burau Grain, E. E., & Cedeño Moreira, C. L. (2026). La importancia de la alfabetización mediática en la era digital: Cómo evaluar la credibilidad de las fuentes de información. *Educational Regent Multidisciplinary Journal*. https://estrellaediciones.com/index.php/educational_regent/article/view/225
- Button, M., Shepherd, D., et al. (2025). Fear of fraud amongst older adults: A hidden epidemic? *Security Journal*. <https://doi.org/10.1057/s41284-025-00485-1>

- Cai, M., Hassan, M. S., & Faizal, S. B. (2024). Information verification behavior in the age of social media: A study of news media literacy against false news. *Journal of Communication*, 28(2), 322–334. <https://doi.org/10.48047/fjc.28.02.17>
- Cha, J. (2024). Predictors of the credibility of social media as a news outlet: An examination of the influences of social media contacts, source perceptions, and media use. *The International Journal on Media Management*. <https://doi.org/10.1080/14241277.2025.2481826>
- DeLiema, M., Gao, S., Brannock, D., & Langton, L. (2025). The effects of risky behaviors and social factors on the frequency of fraud victimization among known victims. *Innovation in Aging*, 9(2), igae111. <https://doi.org/10.1093/geroni/igae111>
- Englander, M., & Morley, J. (2021). Phenomenological psychology and qualitative research. *Phenomenology and the Cognitive Sciences*, 22(1), 25–53. <https://pmc.ncbi.nlm.nih.gov/articles/PMC8556824/>
- Gabor, E. F. G., & Montillano, A. C. (2025). Readiness of Pamantasan Ng Cabuyao education graduates in the licensure examination for teachers: Basis for intervention program. *Jurnal Inovasi Pendidikan*, 3(3), 309–325. <https://doi.org/10.60132/jip.v3i3.535>
- GSMA. (2025, November 13). Rising scam exposure in the Philippines underscores need for cross-sector action, warns new GSMA report. <https://www.gsma.com/newsroom/press-release/rising-scam-exposure-in-the-philippines-underscores-need-for-cross-sector-action-warns-new-gsma-report/>
- Houtti, M., Roy, A., et al. (2024). A survey of scam exposure, victimization, types, vectors, and reporting in 12 countries. *Journal of Online Trust and Safety*. <https://arxiv.org/abs/2407.12896>
- Joseph, A., Fernández, V., et al. (2022). COVID-19 misinformation on social media: A scoping review. *Cureus*. <https://www.cureus.com/articles/94586-covid-19-misinformation-on-social-media-a-scoping-review>
- Moore, D., & Hancock, J. T. (2022). Older adults and susceptibility to fake news: The role of digital literacy. *PLoS ONE*, 17(6), e0269873. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8994776/>

- Moustakas, C. (1994). Phenomenological research methods. Sage Publications.
<https://www.thetbs.org/study-materials/wp-content/uploads/2023/03/Phenomenological-Research-Methods-by-Clark-E.-Moustakas.pdf>
- Parti, K., Tahir, F., & Teaster, P. B. (2025). The wisdom of the scammed: Redefining older fraud victim support by utilizing the ecological systems framework. Security Journal.
<https://doi.org/10.1057/s41284-025-00487-z>
- Perianayagam, A., Bloom, D. E., Lee, J., Parasuraman, S., Sekher, T. V., Mohanty, S. K., Chattopadhyay, A., Govil, D., Pedgaonkar, S., Gupta, S., Agarwal, A., Posture, A., Weerman, A., & Pramanik, S. (2022). Cohort profile: The Longitudinal Ageing Study in India (LASI). *International Journal of Epidemiology*, 51(4), e167–e176.
<https://doi.org/10.1093/ije/dyab266>
- Potter, W. J. (2004). Theory of media literacy: A cognitive approach. Sage Publications.
https://sk.sagepub.com/book/mono/theory-of-media-literacy/toc#_
- Rasi, P., Vuojärvi, H., & Rivinen, S. (2021). Promoting media literacy among older people: A systematic review. *Adult Education Quarterly*, 71(1), 37–54.
<https://doi.org/10.1177/0741713620923755>
- University of Nevada, Reno. (2023). How are deepfakes dangerous?
<https://www.unr.edu/nevada-today/news/2023/atp-deepfakes>
- Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.
<https://rm.coe.int/information-disorder-report-november-2017/1680764666>