Journal homepage: http://pcijournal.org/index.php/ijcss

International Journal of Cultural and Social Science

Published: Pena Cendekia Insani

The Psychological Impact of Digital Fraud: A Phenomenological Study of Victims Impersonating PT Bank Rakyat Indonesia

Salsabila Tita Sukmana[1], Azwar[2]
[1,2]Universitas Pembangunan Nasional "Veteran" Jakarta

Article Info

Keywords:

Banking communication,
Digital fraud,
Digital literacy,
Phenomenology,
Trust

ABSTRACT

Digital fraud impersonating PT Bank Rakyat Indonesia (BRI) has become an alarming phenomenon that causes financial and psychological harm to victims. This study explores victims' lived experiences using a phenomenological approach within a qualitative framework through in-depth interviews and social media observations. The findings show that victims experienced not only financial loss but also emotional distress such as panic, trauma, and a decline in trust toward banking institutions. These experiences influenced how victims interpret digital communication, fostering skepticism toward online information. The phenomenological analysis reveals that meaning is constructed through the interaction of language, past experiences, and awareness of new realities after the fraud. The study emphasizes the need for digital literacy, empathetic communication, and preventive education from financial institutions to restore public trust and strengthen resilience against cybercrime.

Corresponding Author:

Salsabila Tita Sukmana
Ilmu Komunikasi
Universitas Pembangunan Nasional "Veteran" Jakarta
2210411299@mahasiswa.upnvj.ac.id

1. INTRODUCTION

Indonesia's unstable financial situation has led people to justify any means to obtain income. Crime is unavoidable [1]. Between 2024 and 2025, reports recorded more than 274,000 cases of digital fraud impersonating financial institutions an alarming increase of over one hundred percent compared to the beginning of the decade [2]. Customers defrauded by these individuals have suffered significant losses and undermined public trust in the government, banks, and the state. The losses reached 5.7 trillion rupiah. Currently, insecurity arises in many people due to the rise of digital crime, so the co-managed sector is slowly losing public trust because it is considered incapable of guaranteeing adequate protection [3]. The convenience brought by digital banking services actually opens new loopholes, such as the perpetrators are easier to carry out actions because they take advantage of the reputation of official institutions and process psychological manipulation through fraudulent messages, fake service accounts, to sites that are deliberately designed to resemble real bank portals [4] In Indonesia, Bank Rakyat Indonesia (BRI) has millions of customers targeted by fraudsters [5]. Bank names and symbols are misused by digital criminals, such as through phishing emails, fictitious promotions, and credible social media campaigns [6]. The action was not carried out randomly but each message was placed in a planned manner to trigger emotions, curiosity, and the impulse to act quickly from the potential victim [7]. Fake links are used as a means of entry, such as when some victims are lured in large prizes, while others are intimidated by the information that their accounts will be frozen if they do not confirm immediately [8].

With just one click, fraudsters have access to the victim's phone and personal data wide open, resulting in huge losses and misinformation making it difficult for the psychological wounds of the victim to go away [9].

Many of them experience anxiety, deep stress, guilt, and even traumatic symptoms after losing their money and self-esteem [10]. The shame of being deceived results in withdrawal from the environment and triggers a deterioration in mental state [11]. Trust in digital financial services has also begun to decline, creating wider doubts in society [12]. Rebuilding trust is not easy, as bad experiences leave a sense of disappointment at the promise of security that turns out to be not strong enough [13]. The situation is even worse in areas with low digital literacy because people are often unable to distinguish between official and fake messages [14]. A well-known institution's logo or formal sentence alone is enough to convince the victim and immediately believe [15]. Scammers understand the victim's mindset and take advantage of it because they first check the victim's balance amount before committing his crimes [16]. This phenomenon shows that society is less critical because feelings are used more than logic. The lack of media literacy makes misleading information circulate uncontrollably, creating widespread fear [17].

The unpreparedness of the security infrastructure magnifies the opportunity for fraudsters. Under-optimal technology causes fraudsters to have opportunities without many obstacles [18]. Although awareness campaigns have been widely disseminated, the focus is only on technical warnings and does not touch the emotional aspects of the victims. As a result, victims often feel they do not have the support they deserve [19]. Fraud in the digital world is not only a technological problem, but also in the interaction and experience of the customers themselves. So it is important to know how the perspective of the fraud victim after the incident is natural so that a solution can be provided [20]. The phenomenological approach can help explain the case more clearly, as it focuses on the victim's direct experience. In this way, the victim will be more open when giving testimony and this approach can also help his mental and psychological condition [21]. Through a phenomenological approach, researchers can find out the emotional side, thought process, and way the victim communicates about the events they experience [22]. The approach asserts that understanding reality from the victim's point of view is far more important than relying on theories or assumptions of banking institutions.

The Indonesian government and the public are currently finding it difficult to deal with increasing cases of online fraud. Fraud cases are considered like drug abuse because the occurrence is widespread throughout Indonesia. It is caused by a weak security system so that it is easier to commit fraud. When fraud victims reported their fraud cases, the victim only received minimal responses so that they felt ignored by the relevant institutions. Minimal response is the cause of the victim experiencing mental stress and trauma [23]. If the bank or related parties provide empathy and provide information and solutions to the victim properly, the victim will get a sense of security and his emotional problems will heal faster. Therefore, it can be concluded that it is important for relevant institutions to be able to communicate well in responding to the emotions of victims so that public trust becomes better [24]. The types of online fraud and the techniques used are increasingly religious in taking the victim's money and assets. However, the phenomenological approach in understanding the victim's experience is still not widely used. Therefore, discussions about digital fraud must be carried out in depth so that it is not only considered taboo and does not become a case that is never solved.

The rapid development of digital crime and the magnitude of the emotional effects it causes, strengthening cybersecurity is not enough. There is also a need for deeper research on how victims learn from their experiences, both in terms of communication, perception, and emotional processes which are important parts so that recovery is carried out optimallyl [25]. However, an understanding of human communication, perception, and emotional healing is needed to have more impact. This research is important to encourage digital literacy and re-foster trust in Indonesia's financial sector. Through research on the subjective experiences of victims, they can provide insight into a broader crisis of digital trust [26]. The limitations of technology and the lack of state attention make the community more vulnerable. Consumer protection in the financial sector is also still not a priority [27]. Therefore, this research is here to close the literature gap while offering practical guidance for banks, governments, and digital educators to be able to build more empathetic communication, restore victims' psychology, and improve public trust in the digital ecosystem.

2. RESEARCH METHOD

Through a phenomenological perspective in qualitative research, this study aims to explore in depth how customer data leaks can occur and how irresponsible parties use them. Through this approach, it is hoped that a more complete understanding of the root of the problem of misuse of bank consumer information .[3]. To assess the trauma experienced by victims of fraud, reconstruction is necessary to restore customer trust [27]. The trauma experienced by victims is managed effectively to stabilize their emotions and allow for relaxation, allowing for a gradual resolution of the trauma [28]. The victims ranged in age from 17 to 50. Participants in this study were selected using purposive sampling. [29]. Participants in this study were selected using purposive sampling. Informants were required to be active users of digital banking services, including BRI, and to have a history of being victims of digital fraud [30]. In-depth interviews were conducted with victims who were willing to be involved, so that researchers could obtain an in-depth and thorough explanation as the basis for analysis for results and discussion [32]. To make the results of the study more accurate, the researcher conducts a thorough analysis of the informant by examining the data and presenting it in a detailed narrative to ensure that the data tested is valid [34]. Through a phenomenological approach, information is presented in a structured manner so that solutions to problems are easier and in accordance with the conditions of customers who experience fraud.

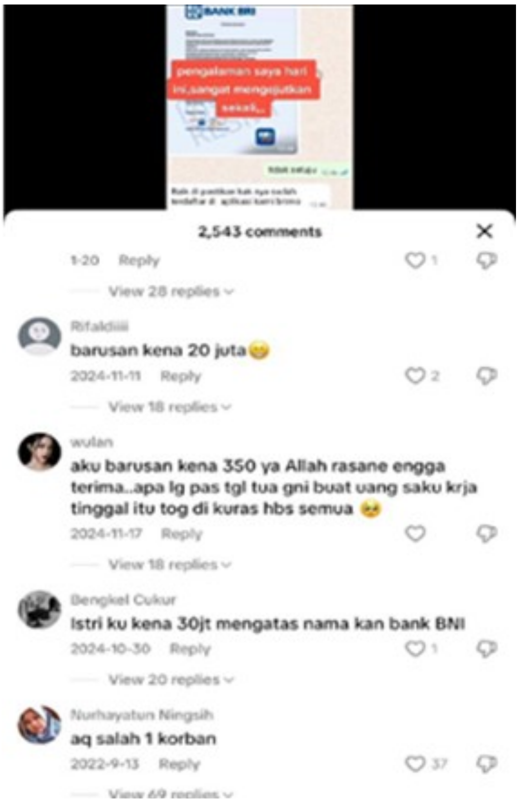
3. RESULT AND ANALYSIS

This study involved two participants who were victims of digital fraud impersonating PT Bank Rakyat Indonesia (BRI). Participants varied in age (21–25 years) and background student, providing diverse perspectives on the psychological, financial, and behavioral impacts of the fraud. Data analysis was conducted through a six-phase thematic analysis following Braun and Clarke (2021), consisting of data familiarization, initial coding, theme generation, theme review, theme definition, and narrative synthesis. Themes were derived inductively from recurring experiences and cross-validated through triangulation of interviews, social media observations, and document analysis to ensure validity and consistency.

Social Media Observation

TikTok, WhatsApp, and Instagram are the platforms used in fraud. Through these platforms, scammers carry out phishing and social engineering. The platform has become a scam suggestion due to its users who easily trust the visual appearance and personal narrative shared by others [35].

The attached image is a TikTok upload belonging to @bundaarkhan04 account. In the video, it is shown how the perpetrator uses the official BRI logo and the communication style made very similar to the bank to convince potential victims. To maintain visual clarity, images are taken directly from the original upload in high quality, without including additional elements such as clocks, signal icons, or other interface displays to keep the focus on the content.



pengalaman saya hari ini,sangat mengejutkan sekali,,

2,543 comments

1-20 Reply 1

View 28 replies

Rifaldiiii
barusan kena 20 juta 😬
2024-11-11 Reply 2

View 18 replies

wulan
aku barusan kena 350 ya Allah rasane engga terima..apa lg pas tgl tua gni buat uang saku krja tinggal itu tog di kuras hbs semua 😖
2024-11-17 Reply

View 18 replies

Bengkel Cukur
Istri ku kena 30jt mengatas nama kan bank BNI
2024-10-30 Reply 1

View 20 replies

Nurhayatun Ningsih
aq salah 1 korban
2022-9-13 Reply 37

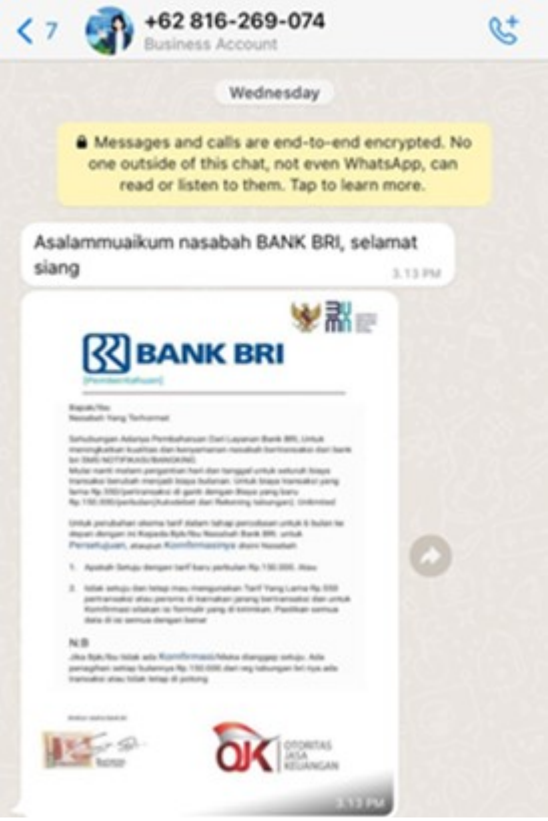
View 69 replies

Figure 2. TikTok Observation
(Source: TikTok @bundaarkhan04)

This condition is in line with the Financial Services Authority (OJK),2024), which recorded a 32% increase in social engineering-based fraud cases throughout 2024. The majority of these criminal acts take place through social media and instant messaging applications, indicating that perpetrators are increasingly adept at combining technology and psychological strategies to trap people [36].

Victims' Subjective Experiences: Fraud Chronology

Based on interviews that have been conducted, scammers are experts in manipulating messages to make them look official. The message sent via WhatsApp was complete with the bank logo, neat writing, and polite, so that the victim of the message was official from Bank BRI directly. This is in accordance with the theory of social proof described in [37] If people believe the information is valid if it comes from an official institution. But the victim did not confirm further whether the message was genuine, not just from the appearance. This technique is known as phishing, where fraudsters fabricate it by taking advantage of the victim's tendency to be trustworthy, especially when the message is made as if urgent [38].



+62 816-269-074
Business Account

Wednesday

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Asalammuaikum nasabah BANK BRI, selamat siang 3.13 PM

BANK BRI

[illegible]

N.B

[illegible]

OJK OTORITAS JASA KEUANGAN

3.13 PM

Figure 3. Fake WhatsApp Message Impersonating BRI

Even though the number used does not come from BRI's official business account, the use of the logo and name of the institution is able to produce strong credible thoughts. The appearance of the message is so similar to the original notification from the bank that the general user has a hard time distinguishing between which is true and which is false. This phenomenon shows that perpetrators use the power of institutional symbols and brand image to gain legitimacy. Many victims judge the authenticity only of the visual elements of the logo, formal format, or delivery style without conducting technical verification.

Therefore, manipulation not only works at the information level, but also utilizes psychological mechanisms. Many customers immediately believe when there is a logo or appearance that looks official because the brain automatically concludes that the message is trustworthy. This sense of trust is used by fraudsters, especially people who do not have good digital literacy. Customers with less digital literacy will have difficulty in ensuring that the information is authentic, such as checking with official contacts and paying attention to the web address listed. Therefore, digital literacy needs to be improved so that customers are more critical in ensuring that the visuals and symbols are fraudulent [39].

Psychological and Emotional Impact on Victims

Victims of digital crime not only lose money, but also experience serious emotional and psychological impacts. Many of them immediately show body reactions such as trembling, shortness of breath, intense panic, and a drastically increased heart rate when they realize that they have been the target of fraud. Shock only arises when the customer has been consciously deceived by causing chest tightness, trembling hands, and abnormal heart rate frequency. This condition is severe stress after people experience danger. Post-traumatic conditions can be identified by the appearance of fear, guilt, and loss of confidence [40]. The victim also felt ashamed and blamed himself for being caught off guard, even though the information provided by the fraudster was very convincing. The strength of the psychological impact can be seen through expressions such as "I was so panicked, my hands were shaking". Victims are convinced to be careful, but in reality they are still deceived, making their confidence decrease and making digital interactions scary. In addition, anxiety increases when there is a fear that personal data is also stolen. Concerns about possible data leaks can trigger anxiety and make a person feel less secure when using digital services [41].

Trust Crisis Toward Banking Institutions

Trust in BRI decreased after experiencing fraud even though the victim also knew that the fraud was not committed by the bank. The victim hopes that the bank should be more active in maintaining customer safety. According to [42], Trust in banking institutions is very volatile because customers depend on how banks act when problems occur. The attitude of banks that are considered less agile makes customers doubt whether to continue to use bank services with a much higher level of vigilance. This condition confirms that digital security issues are not only related to systems or technology, but also involve feelings, social responses, and psychological aspects of users [43]. In order for trust to be restored, banks need to convey information in a more understandable way, educate about fraud, and show empathy to victims. Through this approach, the risk of fraud can be reduced and declining trust can be rebuilt.

Changing Attitudes Toward Digital Information

The way victims respond to digital messages changed drastically after the fraud incident. Now, victims of fraud are more suspicious and double-check when they receive information. This shift in mindset shows that they are starting to interpret every piece of information more carefully, questioning the intent and authenticity of the source. This attitude is in line with the concept of critical digital literacy explained by [44] where users are required to be able to assess the intention, credibility, and context of each information received.

Their perspective on social media is also no longer the same. Social media platforms are no longer used as the main reference to find the truth and are only an additional resource. They just do verification directly through official services such as BRImo or the bank's website before trusting anything. This change in thinking shows the ability to change and adjust after a bad experience as a form of cognitive resilience as described in[45].

Phenomenological Analysis: Meaning-Making of Victims' Experiences

Based on Gadamer's phenomenological perspective, victims have changes in receiving information. In the past, all messages using the bank's logo and name were considered official information, but after experiencing fraud, customers became more careful and double-checked. According to Gadamer, the process is a combination of old experience with a new understanding after the incident occurred [46]. When they found out that their Rp150,000 was missing, the point became a big blow. Although the nominal amount is small, the incident has lowered their trust in the digital world. In phenomenological terms, this can be thought of as the collapse of one's "world" when basic beliefs about technology and the online environment are suddenly no longer safe [47].

Reactions such as trembling hands, panic, and insecurity are not just momentary emotions, but manifestations of inner turmoil as the usually familiar digital space turns into something unsettling.
So, this experience is not just about lost money. More than that, victims feel a major change in the way they see and feel the digital world, such as the condition when a person feels that a place that was once safe is suddenly no longer trustworthy. This phenomenon describes what is referred to as existential dislocation [48].

Reconstruction of Meaning and Adaptive Strategies

Victims become more skeptical after being deceived as a self-protection strategy. Based on Gadamer's perspective, it is the application of life experience to a new context that produces wisdom from bitter experiences (Gadamer, 1975/2021). Victims no longer trust bank advertisements on social media without official verification and support education through channels such as SMS, ATMs, and app notifications. The change marks a shift from passive customers to more critical and active.

Digital Literacy and Critical Public Awareness

The rise of fraud in the digital space encourages each individual to improve their ability to understand information as the main deterrent. Digital literacy skills are very important to avoid cyber fraud in the post-truth era. The problem of digital fraud in Indonesia is very high because people do not have high digital skills so they are vulnerable to fraud. The rise of fraud in the digital space encourages each individual to improve their ability to understand information as the main deterrent. Digital literacy skills are very important to avoid cyber fraud in the post-truth era. The problem of digital fraud in Indonesia is very high because people do not have high digital skills so they are vulnerable to fraud

A large number of people only judge information from its appearance, such as the logo of the institution, neat design, and the use of colors that are professionally considered official information. Psychologically, this thought bias is used by fraudsters because it is only used as the only benchmark. This phenomenon shows that aesthetic and emotional information can influence thinking. Causing difficulties in processing this information is fact or fabricated. Therefore, the ability to imprint literacy is very important for people to use technology safely.

4. CONCLUSION

Victims of digital fraud—particularly scams impersonating banks such as PT Bank Rakyat Indonesia (BRI) experience not only financial losses but also profound psychological and emotional distress. Sophisticated social engineering tactics exploit victims' trust, fear, and sense of urgency through fake WhatsApp messages and other digital channels that mimic official institutions. The findings of this study reveal that the victims' experiences are characterized by anxiety, guilt, and a deep erosion of trust in digital systems, aligning with the study's objective to uncover the subjective meanings and emotional responses within the phenomenological context of digital fraud. This illustrates that fraud victimization in Indonesia is not merely a financial incident but a psychosocial crisis that disrupts individuals' confidence in both technology and institutional authority. Based on these insights, the study recommends a set of practical and context-specific strategies. First, banks and government agencies should establish joint digital literacy programs designed to address the distinct needs of various demographic groups, particularly youth and first-time digital banking users. Financial institutions such as BRI should enhance customer engagement through empathetic and transparent communication, integrating emotional support services such as post-fraud counseling or recovery assistance. Additionally, community-based awareness initiatives—including interactive workshops, social media campaigns, and collaboration with educational institutions—should be developed to improve critical understanding of digital communication cues and fraud prevention. Regulators like OJK and Kominfo are encouraged to create standardized response protocols that ensure victims receive consistent, non-judgmental, and timely assistance, thereby reducing secondary victimization.

This research contributes to existing knowledge by filling a critical gap in understanding the psychological impact of digital fraud in Indonesia, where most studies focus predominantly on technical or financial dimensions. By adopting a phenomenological approach, this study advances the discourse on digital fraud from a purely cybersecurity issue toward a multidimensional phenomenon involving emotion, communication, and trust reconstruction. It provides a framework for future research to explore how emotional resilience and digital empowerment can jointly strengthen user protection in online financial ecosystems. These findings underscore the urgent need to address structural weaknesses in public digital literacy and institutional response. As digitalization accelerates nationwide, the human aspect—particularly empathy, education, and psychological recovery—must be prioritized alongside technological safeguards. Ultimately, this study emphasizes that preventing digital fraud is not only about securing systems, but also about restoring humanity, trust, and confidence in the country's evolving digital economy.

5. REFERENCES

[1] T. Andriyanto, "Komunikasi Termediasi Penipuan dengan Modus Business Email Compromise," *J. Ris. Komun.*, vol. 5, no. 2, pp. 220–243, 2022.

[2] H. AbouGrad and L. Sankuru, "Online Banking Fraud Detection Model: Decentralized Machine Learning Framework to Enhance Effectiveness and Compliance with Data Privacy Regulations," *Mathematics*, vol. 100, no. 13, pp. 1–19, 2025.

[3] A. H. Husna and D. Mairita, "Gen Z dan Perilaku Konsumsi Konten Influencer pada TikTok," *J. Ris. Komun.*, vol. 7, no. 1, pp. 86–100, 2024.

[4] S. Sadeghpour, "Ads and Fraud : A Comprehensive Survey of Fraud in Online Advertising," *J. Cybersecurity Priv.*, vol. 45, no. 76, pp. 804–832, 2025.

[5] H. I. Ma'ruf and A. S. Purnomo, "Analisis Kinerja Pegawai Dengan Pendekatan Fenomenologi Untuk Meningkatkan Kualitas Layanan Paspor Di Kantor Imigrasi Kelas I Non TPI Jakarta Pusat," *Pendas J. Ilm. Pendidik. Dasar*, vol. 9, no. 2, pp. 1–10, 2024.

[6] C. Degeneve, J. Longhi, and Q. Rossy, "Distinguishing Sellers Reported as Scammers on Online Illicit Markets Using Their Language Traces," *Languages*, vol. 9, no. 7, pp. 1–22, 2024.

[7] A. H. Hasanah and O. A. Ismail, "Analisis Semiotika Roland Barthes Mengenai Ketidakadilan Gender Dalam Film Yuni," *J. Ilm. Glob. Educ.*, vol. 4, no. 2, pp. 1000–1010, 2023.

[8] A. Sahfitri and Rosmalinda, "Penipuan Digital Melalui Tautan Phishing," *J. Dialekt. Huk.*, vol. 6, no. 2, pp. 92–107, 2024.

[9] S. N. Fauzi and L. Primasari, "Tindak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli Online (E-Commerce)," *Recidive*, vol. 11, no. 19, pp. 367–386, 2025.

[10] D. O. Aroyo, K. A. Putri, and S. P. Shakira, "Peran Literasi Digital Dalam Menanggulangi Berita Hoaks: Studi Kasus Penipuan Gebyar Hadiah," *Media Digit. Vol.01 No.01 Bulan Mei, Tahun 2025*, vol. 1, no. 1, pp. 60–72, 2025.

[11] L. Mahya, Tarjo, Z. M. Sanusi, and F. A. Kurniawan, "Intelligent Automation Of Fraud Detection And Investigation: A Bibliometric Analysis Approach," *J. Reviu Akunt. dan Keuang.*, vol. 13, no. 3, pp. 588–613, 2023.

[12] A. Reynaldi, M. A. Sunggara, and Y. Meliana, "Analisis Sosiolegal terhadap Dampak Penipuan Online Bagi Masyarakat (Studi Kasus di Wilayah Hukum Pangkalpinang)," *Unes Law Rev.*, vol. 7, no. 2, pp. 816–822, 2024.

[13] M. Anan, S. A. Rahmah, and Risuhendri, "Meningkatkan Kesadaran Digital Dalam Pencegahan Penipuan Online Untuk Kelompok UMKM Desa Tanjung Haratan," *J. Pengabdi. Kpd. Masy.*, vol. 1, no. 1, pp. 56–63, 2024.

[14] N. Baisholan, J. E. Dietz, S. Gnatyuk, M. Turdalyuly, E. T. Matson, and K. Baisholanova, "A Systematic Review of Machine Learning in Credit Card Fraud Detection Under Original Class Imbalance," *Computers*, vol. 14, no. 10, pp. 1–23, 2025.

[15] H. T. Luong and H. M. Ngo, "Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective," *Laws*, vol. 16, no. 12, pp. 1–15, 2024.

[16] M. Siagian *et al.*, "Peningkatan literasi keamanan digital untuk mencegah penipuan online pada pengrajin kayu di Boyolali," *Community Transform. Rev.*, vol. 1, no. 1, pp. 34–45, 2025.

[17] D. P. Kussanti, Susilowati, R. Palupi, and D. T. Bugov, "Politainment Dalam Debut Awal Politik Kaesang Pangarep Terhadap Preferensi Warga Depok," *J. Trias Polit.*, vol. 7, no. 2, pp. 340–358, 2023.

[18] S. Kholmukhammedov, "Cognitive Dissonance: Roles In Contradiction In Consciousness," *World Econ. Financ. Bull.*, vol. 42, no. 1, pp. 186–196, 2025.

[19] T. L. Lombu, "Analisis Nilai-nilai Kepemimpinan Salawa Hada (Kepala Adat): Upaya Membangun Kontekstualisasi Kepemimpinan Kristen Di Kabupaten Nias Selatan," *Sahala J. Manaj. DAN Kepemimp. Kristen*, vol. 1, no. 2, pp. 37–50, 2024.

[20] Y. Rohayati, "Digital Transformation for Era Society 5 . 0 and Resilience : Urgent Issues from Indonesia," *Societies*, vol. 14, no. 1, pp. 1–16, 2024.

[21] W. Gaviyau and J. Godi, "Banking Sector Transformation: Disruptions, Challenges and Opportunities," *FinTech*, vol. 4, no. 3, pp. 1–27, 2025.

[22] A. U. Satira and R. Hidriani, "Peran Penting Public Relations Di Era Digital," *SADIDA*, vol. 1, no. 1, pp. 179–202, 2021.

[23] A. Muftitama, "Perilaku Komunikasi Pada Masyarakat Cyberspace (Netnografi meme rage comic di Situs 1cak.com)," *J. Pikma Publ. Media Dan Cine.*, vol. 5, no. 2, pp. 288–303, 2023.

[24] N. Poernamasari, "Impersonation dan Dark Jokes sebagai Tindakan Cyberbullying dalam Fenomena Bahasa 'Anak Jaksel' di Media Sosial Twitter," *J. Soc. Cult. Lang.*, vol. 2, no. 1, pp. 104–110, 2023.

[25] Z. I. Ajwa, A. Patel, and A. Moseley, "Harnessing AI Technologies: Innovations in Literacy Libraries for Diverse Learners," *Int. J. Cyber IT Serv. Manag.*, vol. 4, no. 1, pp. 19–26, 2024.

[26] S. N. Achmad, “Responsivitas Pelayanan Publik di Era Digital: Evaluasi Peran Institusi dalam Penanganan Cyber Sexual Harassment (Studi Kasus Grup Facebook "Fantasi Sedarah”),” *Parlem. J. Stud. Huk. dan Adm. Publik*, vol. 2, no. 2, pp. 70–91, 2025.

[27] I. Purwata, “Perancangan Alat Penangkap Gambar Pelaku Kejahatan Berbasis Node MCU ESP32 CAM,” *Jambura J. Electr. Electron. Eng.*, vol. 5, no. 1, pp. 36–40, 2023.

[28] P. Priyana, “Alat Bukti Informasi Elektronik Tindak Pidana Penipuan Online Dalam Persfektif Hukum Acara Pidana Di Indonesia,” *J. Ius Kaji. Huk. dan Keadilan*, vol. 9, no. 1, pp. 1–20, 2021.

[29] Z. Abdussamad, *Metode Penelitian Kualitatif*, 1st ed. Bandung: CV. syakir Media Press, 2021.

[30] S. Q. A’yun, B. A. Habsy, and M. Nursalim, “Model-Model Penelitian Kualitatif: Literature Review,” *J. Penelit. Ilmu Pendidik. Indones.*, vol. 4, no. 2, pp. 341–354, 2025.

[31] Sugiyono, *Metode Penelitian Kuantitaif, Kualitatif, R&D*. Bandung: Alfabeta, 2021.

[32] A. Ultavia, P. Jannati, F. Malahati, Qathrunnada, and Shaleh, “Kualitatif: Memahami Karakteristik Penelitian Sebagai Metodologi,” *J. Pendidik. Dasar*, vol. 11, no. 2, pp. 341–348, 2023.

[33] S. W. Purwanza *et al.*, *Metodologi Penelitian Kuantitatif, Kualitatif, dan Kombinasi*, no. March. 2022.

[34] V. S. Yanti and A. Bajari, “Konstruksi Cantik Dalam Akun Instagram Fenomenologi Merasa Cantik menurut Mahasiswa ‘Unpad Geulis’ dalam Akun Instagram Unpad,” *J. Ranah Komun.*, vol. 3, no. 2, pp. 55–68, 2022.

[35] D. Try, H. Hutabarat, and A. M. Panjaitan, “Penegakan Hukum Tindak Pidana Penipuan Online (Studi Kasus Polres Tanjungbalai),” *Pros. Semin. Nas. Multidisiplin Ilmu Univ. Asahan*, vol. 1, no. 6, pp. 52–59, 2023.

[36] M. Kamran and Maskun, “Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika,” *Balobe*, vol. 1, no. 4, pp. 41–56, 2021.

[37] N. N. Firmansyah, Z. Nufus, and R. M. Raharja, “Kesadaran Masyarakat Dalam Menggunakan Media Sosial Untuk Menghindari Terjadinya Modus Penipuan Online,” *Pros. Semin. Nas. Ilmu Pendidik.*, vol. 1, no. 1, pp. 96–103, 2024.

[38] J. A. R. Simanungkalit, R. Hertadi, and A. ul Hosnah, “Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya,” *Akad. J. Mhs. Humanis*, vol. 4, no. 2, pp. 281–294, 2024.

[39] A. Dianto, W. Adam, and F. Febriansyah, “Analisis Pengaruh Brand Equity, Kualitas Produk dan Kepuasan Pelanggan Terhadap Loyalitas Konsumen Pada Bana Swalayan Di Kabupaten Pasaman Barat,” *Jemsi J. Ekon. Manaj. Sist. Inf.*, vol. 6, no. 2, pp. 601–609, 2024.

[40] H. Siswanto, R. W. Putri, E. Dewi, and F. B. Tamza, “Kejahatan Penipuan Investasi Fiktif Sebagai Refleksi Lemahnya Kedaulatan Penegakan Hukum di Tengah Intervensi Global,” *J. Ilmu Sos. Huk. Al-Zayn J. Ilmu Sos. Huk.*, vol. 6, no. 8, pp. 1789–1799, 2025.

[41] N. S. Ardi and Sukaris, “Analisis Resiko Penipuan Dalam Pembelian Online Di Instagram (Perspektif Konsumen),” *J. Mhs. Manaj.*, vol. 4, no. 2, pp. 109–120, 2023.

[42] Y. J. Prasojo, M. M. Ibrahim, and T. A. Joanida, “Penyuluhan Bahaya Penipuan Online sebagai Bentuk Peningkatan Literasi Digital bagi Masyarakat,” *J. Pengabdi. Nas. Indones.*, vol. 4, no. 2, pp. 420–428, 2023.

[43] Linawati and Andryan, “Penegakan Hukum Tindak Pidana Penipuan Berbasis Online dengan Modus Giveaway di Platform Media Sosial: Studi kasus Polres Tanjungbalai,” *As-Syar’i J. Bimbing. Konseling Kel.*, vol. 6, no. 1, pp. 750–757, 2024.

[44] A. F. C. Manga and F. Dianti, “Akibat Hukum dari Perbuatan Melawan Hukum Terhadap Bank dalam Transaksi Letter of Credit,” *SIGn J. Huk.*, vol. 5, no. 2, pp. 292–311, 2023.

[45] M. Putri, Muhidin, and S. Fatmawati, “Analysis Of Child Protection Law Against Victims (Case Study Of Decision Number: 36/PID. SUS/2023/PN. LBB),” *J. Ruang Huk.*, vol. 3, no. 1, pp. 1–10, 2024.

[46] N. Simatupang and Faisal, “Legal Protection for Children as Victims of Trafficking in Persons,” *IJRS Int. J. Reglement& Soc.*, vol. 4, no. 2, pp. 98–104, 2023.

[47] R. W. Ningsih, R. Al Adawiyah, and A. R. Faristiana, “Perkembangan Teknologi Sebagai Modus Scamming Di Laman Jual Beli Online,” *J. Kaji. dan Penelit. Umum*, vol. 1, no. 3, pp. 117–131, 2023.

[48] D. Mei-, A. T. Pamungkas, A. Muliyono, and N. Lahangatubun, “The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions,” *Delictum J. Huk. Pidana Dan Huk. Pidana Islam*, vol. 1, no. 8, pp. 1–20, 2024.