Sinergi International Journal of Communication Sciences
E-ISSN: 2988-6260
Volume. 3, Issue 4, November 2025
Page No: 259-270

Management of the Cekrekening.id Website as a Supporting Mechanism for Online Transaction Security for the Public

Elizabeth Tawlyn Bogar[1], Suparman[2]
[12]IPB University, Indonesia
Correspondent: elistawlyn00@gmail.com[1]

Received : September 29, 2025
Accepted : November 18, 2025
Published : November 30, 2025

Citation: Bogar, E.T., & Suparman, (2025). Management of the Cekrekening.id Website as a Supporting Mechanism for Online Transaction Security for the Public. Sinergi Interntional Journal of Communication Sciences, 3(4), 259-270.

https://doi.org/10.61194/ijcs.v3i4.928

ABSTRACT: This study examines the operational management of digital fraud report classification on CekRekening.id, a national verification platform administered by the Ministry of Communication and Informatics of Indonesia to enhance online transaction security. The research addresses a clear gap in existing literature, as no prior study has provided an insider, process-level description of how fraud reports are screened, verified, and coordinated with banks through direct participant observation within a government digital service. The objective of this study is to explain the end-to-end workflow of fraud report management and identify key challenges that influence system effectiveness and public adoption. The research employed a qualitative participant-observation method during a three-month internship, supported by informal interviews and documentation review conducted within the institutional verification team. Data were grouped into thematic categories to capture procedures, operational constraints, and user behavior patterns that shaped daily verification work. The findings demonstrate that the platform follows a multi-stage workflow comprising submission, initial screening, verification, bank coordination, and publication, while also revealing critical constraints such as low digital literacy, interface ambiguity, limited staffing, and system performance inconsistencies. These findings highlight gaps between the platform's technical design and real-world operational demands. The study recommends strengthening digital literacy initiatives, enhancing interface clarity, improving system reliability, and expanding inter-institutional collaboration. Overall, this research contributes a unique operational perspective that can guide future improvements in national digital transaction security.

Keywords: Digital Literacy, Online Fraud, Account Verification, Digital Transaction Security, Cekrekening.id.

INTRODUCTION

Digital transactions in Indonesia have expanded rapidly with the increasing use of online marketplaces, mobile banking, and electronic payment systems, resulting in new patterns of consumer risk exposure that require institutional mitigation (Prasad & Rohokale, 2020; Silalahi et al., 2022). The acceleration of digital economic activities influences public dependence on online verification tools, making fraud prevention an essential component of national digital governance

(Barry et al., 2012). As transaction volumes grow, users increasingly face deceptive practices ranging from phishing attempts to fraudulent account transfers, illustrating the need for a robust preventive infrastructure supported by accessible verification platforms (Darma, 2022). This condition demonstrates the urgency for government-led digital monitoring initiatives that safeguard public financial activity in the digital sphere (Mitra, 2010).

Low digital literacy remains one of the dominant factors contributing to the persistence of online financial fraud, as many users lack awareness of the indicators of suspicious activity and fail to verify account legitimacy before making payments (Aulia, 2020). Studies show that digitally inexperienced consumers often trust unverified sellers, making them vulnerable to manipulation in online spaces (Nisrina, 2021). These patterns indicate the critical importance of public education on digital safety, especially in environments where financial interactions occur rapidly and without face-to-face confirmation (Muntazah & Andhikasari, 2022). Without adequate literacy, users become increasingly prone to fraudulent schemes that exploit informational asymmetries (Sawlani & Se, 2021).

CekRekening.id was created to address these vulnerabilities by providing the public with a verification mechanism that identifies bank accounts previously reported for fraudulent activity (Kementrian Komunikasi dan Digital Republik Indonesia, 2020). The platform allows users to check account histories and submit reports accompanied by supporting evidence, enabling the gathering of community-driven fraud data (Prastiwi et al., 2022). As a state-operated tool, the platform integrates digital communication principles that emphasize transparency and trust-building between government and citizens (Rahman & Panuju, 2017). The presence of CekRekening.id reflects an institutional effort to reduce fraud losses by embedding preventive mechanisms directly into public digital behaviors (Rozaq & Nugrahani, 2023).

Previous studies on digital fraud prevention in Indonesia have focused on technological system design, cybersecurity frameworks, and digital literacy interventions, but they rarely address the internal operational dynamics of government verification systems (Putri et al., 2024). While technical studies provide useful insights about algorithmic detection, they overlook the human-driven verification processes that shape the real-world accuracy of fraud classification (Amirillah, 2025). At the same time, communication and digital governance literature highlights the significance of workflow clarity and information flow in public institutions, yet empirical accounts of these processes remain limited (Rahmawati, 2017). This gap underscores the need for an operationally grounded perspective on digital fraud management conducted inside government environments (Adira et al., 2024).

Research on public-facing digital platforms suggests that service reliability depends on the accuracy of user-submitted information, institutional coordination, and system responsiveness, which collectively influence public trust (Cahyani et al., 2024). These studies emphasize that technical quality alone cannot ensure effective adoption without supportive communication mechanisms and intuitive interface design (Raffi & Dianita, 2024; Rizaldi & Hidayat, 2020). Similarly, literature on digital interaction shows that poorly structured user flows contribute to reporting errors and reduce the efficiency of verification teams (Ferica & Parlindungan, 2020). Therefore, understanding the platform's internal processes becomes essential for identifying bottlenecks that limit its preventive role (Riyantie et al., 2021).

CekRekening.id is operated by a specialized verification team within the Ministry of Communication and Informatics of Indonesia, which processes thousands of public reports annually, demonstrating high public reliance on the platform (Lestari & Ali, 2020). However, despite its substantial use, the platform encounters persistent operational issues such as incomplete evidence submissions, duplicated reports, and inconsistent coordination with financial institutions (Octora & Alvin, 2022). These recurring constraints reflect broader challenges faced by digital government services that depend on manual verification and cross-agency collaboration to validate user-generated information (Nursatyo & Rosliani, 2018). Addressing these obstacles requires a deeper understanding of the lived operational realities inside verification institutions (Gunawan, 2020).

Technical barriers such as slow dashboard performance, outdated interface elements, and irregular maintenance schedules further aggravate delays in fraud classification, directly impacting platform responsiveness (Afika & Romli, 2025). These limitations align with findings in usability research stating that unclear system architecture and performance inconsistencies hinder user experience and reduce platform credibility (Cahyono et al., 2023). The documented issues also show that system infrastructure must evolve in parallel with user needs and increasing report volumes to maintain effective fraud prevention (Taqwiym, 2025). As digital platforms scale, responsiveness becomes a critical determinant of public trust (Saputra et al., 2023).

Beyond technical issues, social disparities further complicate platform effectiveness, particularly in regions with uneven internet access and limited digital communication exposure (Kurnianti, 2018). These conditions hinder users from submitting clear and complete evidence, resulting in high rejection rates and reduced verification accuracy (Ri'aeni, 2017). Communication studies emphasize that without targeted outreach campaigns, digital public services will not achieve optimal penetration across diverse socio-economic groups (Muntazah & Andhikasari, 2022). Thus, platform optimization requires not only system improvement but also an inclusive communication strategy (Prastiwi et al., 2022).

The gap between platform potential and operational constraints highlights the need for systematic evaluation of internal workflow processes within CekRekening.id (Prasad & Rohokale, 2020). While the platform is technologically functional, its effectiveness is constrained by user errors, limited human resources, and infrastructural challenges that shape verification outcomes (Silalahi et al., 2022). Existing research has not addressed these process-level issues, thereby creating a theoretical and practical void that must be filled through direct observation of daily verification procedures (Aulia, 2020). This study responds to that gap by offering an operational analysis grounded in real institutional practice (Barry et al., 2012).

This research seeks to answer two primary questions: first, how the end-to-end management of digital fraud report classification is conducted within CekRekening.id; and second, what major constraints hinder its operational effectiveness (Mitra, 2010). The novelty of this study lies in its insider perspective obtained through participant observation during an internship a methodological approach rarely applied in Indonesian digital governance research (Miles et al., 2014). By documenting the workflow, communication patterns, and institutional challenges, this study contributes a process-level understanding that complements previous technical and communication-oriented analyses (Cahyono et al., 2023). The insights presented offer a foundation for improving platform reliability, optimizing workflow design, and strengthening national digital transaction security (Darma, 2022).

METHOD

This study employed a qualitative approach using participant observation conducted during a three-month internship within the verification team of the Ministry of Communication and Informatics of Indonesia, enabling a close understanding of operational processes in CekRekening.id (Creswell & Poth, 2018) Gunawan, 2020). Qualitative inquiry enables researchers to capture contextualized interactions and operational meanings that emerge within natural work settings (Miles et al., 2014). This methodological alignment allows the study to obtain rich, process-level insights concerning communication patterns, verification logic, and classification procedures within CekRekening.id (Gunawan, 2020). The insights presented offer substantial empirical grounding that reflects the complexities of decision-making across institutional verification activities (Mahmudah & Rahayu, 2020).

The researcher functioned as an embedded participant observer, engaging directly in verification tasks while documenting interactions, decision sequences, and operational constraints (Adira et al., 2024). This design reflects a single-case, process-tracing qualitative study that focuses on institutional procedures applied within a specific digital public service (Prasad & Rohokale, 2020). As an embedded observer, the researcher gained systematic access to the internal workflow of CekRekening.id, a methodological contribution rarely adopted in studies of digital complaint systems (Rozaq & Nugrahani, 2023). The combination of immersion, iterative reflection, and collaborative learning provided contextual depth that enhances the analytical rigor of the study (Cahyono et al., 2023).

The research population consisted of team members directly involved in handling public submissions through CekRekening.id within the Ministry of Communication and Informatics of Indonesia (Kementrian Komunikasi dan Digital Republik Indonesia, 2020). The researcher interacted with approximately one team leader, several verification officers, and IT support personnel responsible for system maintenance and dashboard performance (Silalahi et al., 2022). These personnel represented the core operational actors who determine classification accuracy, manage report flows, and maintain data integrity (Darma, 2022). The sampling technique was purposive, ensuring that each informant contributed information relevant to the research focus on workflow management and operational constraints (Mahmudah & Rahayu, 2020).

Informal interviews were conducted to gather insights into verification routines, technological challenges, and coordination with financial institutions, strengthening the contextual interpretation of observed activities (Mitra, 2010). Ethical considerations were addressed through institutional permission, confidentiality assurances, and the anonymization of informant identities throughout documentation (Barry et al., 2012). The purposive selection of informants allowed the study to align data collection with the research questions concerning process efficiency and constraint identification (Lestari & Ali, 2020). This combination of observation, ethical compliance, and targeted engagement enhanced the credibility of the findings (Saputra et al., 2023).

The study was conducted at the Ministry of Communication and Informatics of Indonesia within the directorate responsible for electronic transaction supervision, which manages all operational activities related to CekRekening.id (Prastiwi et al., 2022). The office environment provided direct access to internal dashboards, verification tools, and procedural documentation necessary for understanding system functionality (Cahyani et al., 2024). The strategic location facilitated real-time observation of workflow sequences, evidence assessments, and communication exchanges among verification officers (Aulia, 2020). This environment ensured that the researcher could observe authentic operational patterns that shape fraud-report classification outcomes (Silalahi et al., 2022).

The three-month internship allowed the researcher to examine routine and peak operational cycles, including fluctuations in user submissions during high-traffic periods (Riyantie et al., 2021). This duration also enabled longitudinal reflection on repeated issues such as report duplication, incomplete evidence, and inconsistent bank response times (Rahmawati, 2017). The extended engagement strengthened data validity by enabling cross-checking between daily observations and accumulated experiences over time (Miles et al., 2014). Through this process, the study captured changes in team coordination, system reliability, and workflow intensity across multiple operational conditions (Darma, 2022).

This study employed multiple qualitative instruments, including field notes, internal documents, verification dashboards, and institutional communication records (Cahyono et al., 2023). Field notes captured chronological observations, decision pathways, and recurring challenges in evidence interpretation, reflecting the core role of qualitative documentation in understanding natural processes within institutional environments (Creswell & Poth, 2018). Internal documents, such as SOPs and operational guidelines, provided structural insights into the expected verification standards applied within the platform (Adira et al., 2024). Verification dashboards and communication records offered real-time visibility into classification flows, evidence uploads, and officer system interactions (Silalahi et al., 2022). This combination of instruments ensured comprehensive triangulation of behavioral, procedural, and technological aspects of verification work (Barry et al., 2012).

Access to the internal dashboard of CekRekening.id was granted as part of the internship, enabling the researcher to observe classifications, system notifications, and the data lifecycle of each submitted report (Prastiwi et al., 2022). Digital tools, including shared spreadsheets and communication platforms, supported the tracking of report status, bank responses, and verification notes (Kurnianti, 2018). These instruments facilitated continuous comparison between raw evidence and classification outcomes, strengthening analytic reliability (Barry et al., 2012). Documentation practices followed qualitative standards prioritizing accuracy, transparency, and contextual completeness (Creswell & Poth, 2018).

Data collection employed four integrated techniques: participant observation, involvement in verification activities, informal interviews, and literature review (Mitra, 2010). Participant observation allowed the researcher to record workflow sequences, identification criteria, and evidence assessment steps used by verification officers, providing immersive access to institutional processes (Miles et al., 2014). Active involvement strengthened understanding of operational logic by engaging directly with system tools and classification procedures used in daily decision-making (Gunawan, 2020). Literature review supported the analytical process by linking observed problems with existing studies on digital governance, communication systems, and fraud-prevention frameworks (Prasad & Rohokale, 2020). This integration of techniques ensured that the generated findings were grounded both in empirical observation and relevant theoretical perspectives (Mitra, 2010).

Informal interviews with verification officers and IT personnel provided context behind ambiguous cases, system interruptions, and cross-agency coordination (Cahyani et al., 2024). These interviews, combined with observational notes, supported methodological triangulation that enhanced data accuracy and interpretive depth (Gunawan, 2020). The researcher recorded recurring themes such as user errors, system delays, and interface challenges that affected classification performance (Ferica & Parlindungan, 2020). The integration of multiple techniques ensured that findings captured both procedural and experiential dimensions of platform management (Rozaq & Nugrahani, 2023).

Data were analyzed using the Miles and Huberman (2014) interactive model, comprising data reduction, data display, and drawing conclusions. Manual coding was conducted iteratively to refine categories and identify recurring operational patterns, following qualitative analytical procedures that emphasize systematic interpretation of field-based evidence (Creswell & Poth, 2018). This process enabled the differentiation between user-generated problems and structural constraints embedded within the verification system (Silalahi et al., 2022). These analytic steps ensured that conclusions were grounded in consistent cross-checking with raw data (Darma, 2022).

Data display involved organizing thematic patterns into narrative summaries and analytic matrices that enabled comparisons across workflow stages and constraint categories (Prastiwi et al., 2022). Continuous verification against raw data ensured analytical consistency and minimized interpretive bias during theme development (Darma, 2022). The final stage of drawing conclusions synthesized core insights regarding process efficiency, verification accuracy, and systemic constraints affecting the platform (Cahyono et al., 2023). This analytical approach supported a comprehensive understanding of how operational factors shape fraud-report classification outcomes (Aulia, 2020).

RESULT AND DISCUSSION

Management of Digital Crime Report Classification on CekRekening.id

The classification process begins when users submit evidence such as screenshots, account numbers, and transaction details through the CekRekening.id online reporting form (Kementrian Komunikasi dan Digital Republik Indonesia, 2020). Each submission is automatically entered into the verification dashboard, where officers assess completeness and relevance as part of the initial screening stage (Silalahi et al., 2022). This early review ensures that only reports containing financial indicators are considered for further processing, such as proof of transfer or documented requests for payment (Rozaq & Nugrahani, 2023). Accurate user submissions significantly affect system efficiency because incomplete reports increase manual workload and delay subsequent workflow stages (Darma, 2022).

During initial screening, officers verify account numbers, categorize report types, and filter submissions that fall outside the platform's mandate, such as personal disputes or non-transactional complaints (Aulia, 2020). Many reports require correction due to blurred screenshots, misinterpreted categories, or insufficient descriptions, leading to early rejection (Ferica & Parlindungan, 2020). This screening step functions as a quality-control filter that preserves data consistency across the verification system (Cahyono et al., 2023). Effective screening is essential to prevent irrelevant reports from entering deeper verification stages that require more administrative effort (Prastiwi et al., 2022).

Reports that pass screening proceed to evidence evaluation, where officers examine transaction proofs, payment confirmations, and conversation logs to determine whether fraud indicators are present (Nursatyo & Rosliani, 2018). Officers cross-check each submission against internal fraud databases and previously reported accounts to identify patterns and detect repeat offenders (Barry et al., 2012). If evidence aligns with criteria for suspicious activity, the case is categorized as verified; otherwise, it is labeled as insufficient and stored for archival purposes (Miles et al., 2014). This evaluation stage ensures that only substantiated cases progress to coordination with financial institutions (Darma, 2022).

Coordination with banks represents the verification stage in which officers forward validated cases to partner financial institutions for confirmation of account ownership or investigative updates (Silalahi et al., 2022). Bank responses vary in speed depending on internal processes, affecting the timeline for case completion (Lestari & Ali, 2020). This cross-agency collaboration ensures that published cases do not falsely accuse legitimate account holders, preserving fairness and data integrity (Prastiwi et al., 2022). Financial institutions serve as authoritative validators, strengthening the accuracy of final classifications (Gunawan, 2020).

After bank confirmation, verified fraudulent accounts are published on the platform, enabling users to check risk indicators before conducting transactions (Kementrian Komunikasi dan Digital Republik Indonesia, 2020). Publication also updates the system's internal fraud repository, supporting future cross-checking and trend analysis (Aulia, 2020). This final stage reflects a transparent communication process between government institutions and the public, enhancing trust in digital security measures (Riyantie et al., 2021). Through this structured workflow, CekRekening.id fulfills its preventive function by providing accessible fraud awareness information to the public (Prasad & Rohokale, 2020).

Constraints in Report Classification Management

User-generated errors constitute a major constraint in the fraud-report classification process, as many submissions lack clear descriptions or fail to include complete evidence (Aulia, 2020). These issues commonly involve screenshots that do not display transaction proof or narrative fields containing vague accounts of events (Mitra, 2010). Such inaccuracies force verification officers to spend additional time reviewing incomplete data or rejecting reports that do not meet the platform's requirements (Ferica & Parlindungan, 2020). High rejection rates demonstrate how user literacy significantly influences system efficiency (Muntazah & Andhikasari, 2022).

System limitations also hinder operational performance, including slow dashboard loading, delayed file rendering, and inconsistent data synchronization (Cahyani et al., 2024). These disruptions reduce workflow continuity by compelling officers to refresh pages or access the system using alternative devices (Silalahi et al., 2022). Technical inefficiencies lower productivity during peak reporting cycles when large volumes of submissions require rapid processing (Darma, 2022). As systems struggle under heavy load, verification accuracy and timeliness are directly affected (Cahyono et al., 2023).

Interface design challenges create additional barriers for users unfamiliar with structured reporting tools (Nisrina, 2021). Confusing evidence-upload instructions and limited field explanations contribute to misinterpretation of reporting steps (Riyantie et al., 2021). On the administrative side, limited filtering and sorting features make it difficult for officers to trace previous submissions or identify report patterns efficiently (Prastiwi et al., 2022). These interface-related issues illustrate how usability affects both user behavior and institutional workflow (Darma, 2022).

Organizational constraints, particularly limited staffing, influence verification speed and overall platform reliability (Lestari & Ali, 2020). The verification team must handle substantial report volumes without proportional increases in personnel, especially during national shopping periods or high-risk seasons (Adira et al., 2024). Weekly coordination meetings provide structured communication, but urgent matters sometimes require immediate responses that exceed available resources (Gunawan, 2020). Staffing imbalances contribute to delays that reduce the platform's responsiveness to public needs (Kurnianti, 2018).

Broader socio-technical factors also affect report quality, especially in regions with limited internet access or low digital literacy (Muntazah & Andhikasari, 2022). Poor connectivity results in blurred evidence uploads or incomplete form submissions, limiting the likelihood that reports meet verification standards (Sawlani & Se, 2021). Users who lack familiarity with digital documentation processes struggle to navigate the reporting interface, increasing the frequency of incorrect submissions (Ferica & Parlindungan, 2020). These disparities underscore the need for inclusive outreach to ensure equitable access to fraud-reporting tools (Prastiwi et al., 2022).

The findings indicate that the CekRekening.id workflow reflects a linear communication process in which user-submitted information must be decoded and reinterpreted by verification officers to determine its accuracy (Barry et al., 2012). Communication studies emphasize that unclear messages introduce noise that disrupts the delivery of meaning between senders and receivers, a condition frequently observed in digital interactions involving incomplete or ambiguous user submissions (Mitra, 2010). This situation aligns with the high rate of unclear evidence found during field observations, which decreases verification efficiency and increases the officer's workload (Aulia, 2020). These communication disruptions highlight how message quality directly affects operational performance within digital fraud-reporting systems (Silalahi et al., 2022).

Technical infrastructure strongly shapes the platform's capacity to deliver timely and accurate classifications (Darma, 2022). System delays, file-rendering issues, and inconsistent synchronization were recurrent obstacles that impeded officers from completing verification tasks efficiently (Cahyono et al., 2023). Platform reliability is a key determinant of public trust, especially for digital services used to support financial safety (Prastiwi et al., 2022). These challenges indicate the need for improved system optimization, automated detection mechanisms, and more responsive maintenance cycles (Putri et al., 2024).

The usability of the reporting interface influences both user participation and data quality submitted to the verification team (Nisrina, 2021). Ambiguous labeling, absent guidance features, and limited instructional clarity encourage user mistakes that increase administrative workload (Riyantie et al., 2021). Research on UI/UX suggests that step-by-step guides, automated quality checks, and clearer evidence-field instructions can significantly reduce errors (Cahyani et al., 2024). Redesigning the interface to reduce confusion enables more effective communication between the public and verification officers (Ferica & Parlindungan, 2020).

The study also highlights how broader socio-technical factors influence the effectiveness of CekRekening.id as a public service (Muntazah & Andhikasari, 2022). Low digital literacy, unstable internet connections, and limited exposure to digital reporting tools contributed to high frequencies of incorrect submissions (Sawlani & Se, 2021). These findings reinforce research indicating that awareness-building strategies and inclusive communication campaigns are essential for digital service adoption (Kurnianti, 2018). Strengthening outreach efforts across local communities can enhance user participation and elevate report accuracy (Lestari & Ali, 2020).

Organizational constraints, particularly limited staffing, contributed to delays in report handling and processing (Adira et al., 2024). Digital service management literature emphasizes that human-resource readiness is critical for high-demand systems, especially those requiring daily decision-making and cross-agency communication (Gunawan, 2020). Improvements in workflow structure, personnel capacity, and real-time coordination mechanisms are required to strengthen operational alignment with increasing report volumes (Prastiwi et al., 2022). Collectively, these insights highlight that effective fraud prevention requires synchronized improvements in interface design, staff allocation, public literacy, and technological infrastructure (Prasad & Rohokale, 2020).

CONCLUSION

This study examined the operational management of digital fraud-report classification on CekRekening.id through qualitative participant observation conducted within the Ministry of Communication and Informatics of Indonesia (Kementrian Komunikasi dan Digital Republik Indonesia, 2020). The findings show that the platform relies on a multi-stage workflow consisting of submission, screening, verification, bank coordination, and publication, reflecting a structured approach to fraud prevention (Silalahi et al., 2022). These stages demonstrate the platform's commitment to transparency, accuracy, and public protection in digital transactions (Aulia, 2020). The study contributes an insider perspective that fills a gap in previous research by documenting the detailed operational processes underlying fraud-report classification (Prastiwi et al., 2022).

Operational constraints identified in this research include user-generated errors, system limitations, interface design challenges, staffing shortages, and socio-technical barriers such as uneven digital literacy (Muntazah & Andhikasari, 2022). These findings emphasize the need for structured interface enhancements, digital literacy initiatives, consistent system maintenance, and expanded staff capacity to strengthen service reliability (Darma, 2022). The study provides a practical roadmap for improving national digital fraud management by integrating technological, organizational, and communication strategies (Cahyono et al., 2023). Strengthening these areas will enhance the preventive impact of CekRekening.id and support safer online financial interactions across Indonesia (Prasad & Rohokale, 2020).

REFERENCES

Adira, M. F., Tambunan, S. A. F., Adelia, P. N., & Ikhwan, A. (2024). Perancangan Sistem Informasi Manajemen Secure Socket Layer pada Website Pemerintah Kota Medan. *Technologia: Jurnal Ilmiah*, *15*(1), 109–120. https://doi.org/10.31602/tji.v15i1.13897

Afika, B. A., & Romli, M. A. (2025). Perancangan Sistem Pembayaran WiFi Berbasis Web dan Mobile sebagai Pendukung Efisiensi Manajemen Layanan Internet. *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *7*(2), 749–758. https://doi.org/10.51401/jinteks.v7i2.5709

Amirillah, C. D. R. (2025). Deteksi Transaksi Penipuan pada Sektor Perbankan Menggunakan Rule-Based Model dan Pembelajaran Mesin. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, *14*(2), 96–102. https://doi.org/10.22146/jnteti.v14i2.17410

Aulia, S. (2020). Pola Perilaku Konsumen Digital dalam Memanfaatkan Aplikasi Dompet Digital. *Jurnal Komunikasi*, *12*(2), 311–324. https://doi.org/10.24912/jk.v12i2.9829

Barry, J. R., Lee, E. A., & Messerschmitt, D. G. (2012). *Digital Communication*. Springer Science & Business Media.

Cahyani, A. A., Kholik, A., & Rizki, M. F. (2024). Optimalisasi Komunikasi Digital dalam Penerapan Visual Sosial pada Desain atau Layout Website Company Profile. *Jurnal Syntax Admiration*, *5*(7), 2447–2461. https://doi.org/10.46799/jsa.v5i7.1303

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design: Choosing among Five Approaches* (4th ed.). SAGE Publications.

Darma, G. S. (2022). Website Usability, Satisfaction, Loyalty, Security Perception, Trust and Word of Mouth in E-Commerce Business. *Jurnal Manajemen Bisnis*.

Ferica, S., & Parlindungan, D. R. (2020). Pemanfaatan Media Sosial Instagram sebagai Strategi Komunikasi Pemasaran pada Online Shop @diet_inget_irwan. *KALBISOCIO Jurnal Bisnis Dan Komunikasi*, *7*(2), 53–58.

Kementrian Komunikasi dan Digital Republik Indonesia. (2020). *110 Laporan Rekening Terindikasi Penipuan Online*.

Kurnianti, A. W. (2018). Strategi Komunikasi Pemasaran Digital sebagai Penggerak Desa Wisata Kabupaten Wonosobo Provinsi Jawa Tengah. *Jurnal Riset Komunikasi (JURKOM)*, *1*(1), 180–190. https://doi.org/10.24329/jurkom.v1i1.24

Lestari, G. T., & Ali, D. S. F. (2020). Strategi Komunikasi Pemasaran Disporaparbud Kabupaten Purwakarta melalui Media Aplikasi Sampurasun dalam Mempromosikan Pariwisata. *Linimasa: Jurnal Ilmu Komunikasi*, *3*(1), 1–10. https://doi.org/10.23969/linimasa.v3i1.2056

Mitra, A. (2010). *Digital Communications: From E-mail to the Cyber Community*. Infobase Publishing.

Muntazah, A., & Andhikasari, R. (2022). Peran Media Digital dalam Strategi Komunikasi Pemasaran Lembaga Filantropi Islam di Indonesia. *JKOMDIS: Jurnal Ilmu Komunikasi Dan Media Sosial*, *2*(1), 1–7. https://doi.org/10.47233/jkomdis.v2i1.53

Nisrina, R. G. (2021). User Generated Content sebagai Strategi Komunikasi Pemasaran Digital: Studi Kasus Fenomena #shopeehaul. *Jurnal Komunikasi Profesional*, *5*(6), 558–571. https://doi.org/10.25139/jkp.v5i6.4316

Nursatyo, N., & Rosliani, D. (2018). Strategi Komunikasi Pemasaran Digital Situs Pembanding Harga Telunjuk.com. *Expose: Jurnal Ilmu Komunikasi*, *1*(2), 46–67. https://doi.org/10.33021/exp.v1i2.430

Octora, H., & Alvin, S. (2022). Strategi Komunikasi Pemasaran Terpadu Digital pada Proses Penerimaan Mahasiswa Baru Untar. *Professional: Jurnal Komunikasi Dan Administrasi Publik*, *9*(2), 261–270.

Prasad, R., & Rohokale, V. (2020). *Cyber Security: The Lifeline of Information and Communication Technology*. Springer International Publishing. https://doi.org/10.1007/978-3-030-31703-4

Prastiwi, N. A., Kholil, S., & Sumanti, S. T. (2022). Pengelolaan Website Dinas Komunikasi dan Informatika Kabupaten Asahan sebagai Akses Informasi Publik. *SIBATIK JOURNAL*, *1*(11), 2605–2614. https://doi.org/10.54443/sibatik.v1i11.399

Putri, N. C. R., Fauzi, A., Ali, M. K., Ramadhan, N. A., Salsabilla, P. J., Cahya, L. J., & Ernawati, F. A. (2024). Strategi Peningkatan Keamanan Data Pelanggan dalam Penjualan Online di Tokopedia. *Jurnal Siber Multi Disiplin*, *2*(1), 54–67. https://doi.org/10.38035/jsmd.v2i1.136

Raffi, M., & Dianita, I. A. (2024). Analisis Strategi Komunikasi Pemasaran @Ninetysixvintages pada Media Sosial Instagram. *Jurnal Pustaka Komunikasi*, *7*(1), 50–63. https://doi.org/10.32509/pustakom.v7i1.3305

Rahman, I. A., & Panuju, R. (2017). Strategi Komunikasi Pemasaran Produk Fair N Pink melalui Media Sosial Instagram. *WACANA: Jurnal Ilmiah Ilmu Komunikasi*, *16*(2), 214–224. https://doi.org/10.32509/wacana.v16i2.26

Rahmawati, M. (2017). Penggunaan Sistem Informasi dalam Komunikasi Bisnis secara Elektronik. *Jurnal Komunikasi*, *8*(2).

Ri'aeni, I. (2017). Strategi Komunikasi Pemasaran Digital pada Produk Kuliner Tradisional. *Lugas Jurnal Komunikasi*, *1*(2), 141–149. https://doi.org/10.31334/ljk.v1i2.443

Riyantie, M., Alamsyah, A., & Pranawukir, I. (2021). Strategi Komunikasi Pemasaran Kopi Janji Jiwa di Era Digital dan Era Pandemi Covid-19. *WACANA: Jurnal Ilmiah Ilmu Komunikasi*, *20*(2), 255–267. https://doi.org/10.32509/wacana.v20i2.1721

Rizaldi, A., & Hidayat, H. (2020). Digital Marketing Communication Strategy. *Jurnal Entrepreneur Dan Entrepreneurship*, *9*(2), 57–66. https://doi.org/10.37715/jee.v9i2.1340

Rozaq, M., & Nugrahani, R. U. (2023). Penggunaan Platform Video Pendek sebagai Strategi Komunikasi Pemasaran Digital untuk UMKM. *Jurnal Komunikasi Nusantara*, *5*(1), 21–30. https://doi.org/10.33366/jkn.v5i1.271

Sawlani, D. K., & Se, M. (2021). *Keputusan Pembelian Online: Kualitas Website, Keamanan dan Kepercayaan*. Scopindo Media Pustaka.

Silalahi, P. R., Daulay, A. S., Siregar, T. S., & Ridwan, A. (2022). Analisis Keamanan Transaksi E-Commerce dalam Mencegah Penipuan Online. *Jurnal Manajemen Bisnis Dan Akuntasi*, *1*(4), 224–235. https://doi.org/10.58192/profit.v1i4.481

Taqwiym, A. (2025). Penerapan Sistem Informasi Berbasis Web dalam Usaha Jasa Penyewaan dengan Perspektif Hukum Perlindungan Data dan Transaksi Elektronik. *Jurnal SIFRA: Jurnal Sistem, Informasi, Dan Rekayasa*, *1*(1), 42–53.