

## PENDAMPINGAN LITERASI DIGITAL DALAM PENCEGAHAN PENIPUAN SIBER MELALUI WEBINAR EDUKATIF

**Feliks Prasepta Sejahtera Surbakti**

Program Studi Teknik Industri, Universitas Katolik Indonesia Atma Jaya, Indonesia  
[feliks.prasepta@atmajaya.ac.id](mailto:feliks.prasepta@atmajaya.ac.id)

### ABSTRAK

**Abstrak:** Pesatnya perkembangan teknologi informasi meningkatkan kasus penipuan digital, khususnya melalui media sosial dan transaksi keuangan daring, sehingga mengancam keamanan masyarakat di ruang siber. Tujuan utama kegiatan ini adalah meningkatkan kesadaran masyarakat terhadap berbagai bentuk penipuan digital serta membekali mereka dengan keterampilan praktis untuk menghindarinya. Metode yang digunakan mencakup webinar publik, distribusi infografis dan video edukatif pendek, serta simulasi pelatihan untuk mengenali dan merespons modus penipuan. Kegiatan ini juga melibatkan kerja sama dengan 2 mitra institusi yaitu Kominfo dan Komisi I DPR RI. Peserta webinar berjumlah 120 orang yang berasal dari wilayah Jakarta Pusat, Jakarta Selatan, serta luar negeri. Hasilnya menunjukkan peningkatan pemahaman peserta yang signifikan sebesar 75%, ditandai dengan kemampuan yang lebih baik dalam mengidentifikasi jenis penipuan digital. Edukasi ini terbukti efektif dalam membangun budaya waspada dan meningkatkan literasi digital masyarakat, sehingga mampu menurunkan risiko menjadi korban penipuan di dunia maya.

**Kata Kunci:** Keamanan Siber; Dunia Maya; Penipuan Digital; Literasi Digital.

**Abstract:** The rapid development of information technology has led to a significant increase in digital fraud, particularly through social media and online financial transactions, thereby posing a serious threat to public security in cyberspace. The primary objective of this activity was to enhance public awareness of various forms of digital fraud and to equip participants with practical skills to avoid such threats. The methods employed included a public webinar, the distribution of infographics and short educational videos, as well as training simulations to recognize and respond to fraud schemes. This activity involved collaboration with two institutional partners, namely the Ministry of Communication and Informatics and Commission I of the Indonesian House of Representatives. The webinar was attended by 120 participants from Central Jakarta, South Jakarta, and overseas. The results indicated a significant improvement in participants' understanding by 75%, as reflected in their enhanced ability to identify different types of digital fraud. This educational initiative proved effective in fostering a culture of vigilance and improving digital literacy, thereby reducing the risk of becoming victims of online fraud.

**Keywords:** Cybersecurity; Cyberspace; Digital Fraud; Digital Literacy.



#### Article History:

Received: 12-12-2025  
Revised : 31-12-2025  
Accepted: 03-01-2026  
Online : 01-02-2026



This is an open access article under the CC-BY-SA license

## A. LATAR BELAKANG

Seiring dengan pesatnya perkembangan teknologi informasi, masyarakat kini semakin terhubung dengan dunia digital. Kemudahan akses informasi, transaksi daring, dan komunikasi global telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Namun, di balik berbagai kemudahan tersebut, terdapat ancaman yang terus berkembang, yaitu penipuan digital di dunia maya (Hendrik S, 2019). Penipuan digital dapat terjadi dalam berbagai bentuk, seperti *phishing*, pencurian identitas, penipuan transaksi, dan berbagai modus lainnya yang dapat merugikan secara finansial maupun merusak reputasi individu serta lembaga (Permatasari et al., 2024).

Di era transformasi digital saat ini, semakin banyak institusi pemerintah yang memanfaatkan teknologi untuk meningkatkan efisiensi pelayanan, namun hal ini juga membuka peluang bagi pelaku kejahatan siber untuk melakukan penipuan digital (Surbakti, 2024). Menurut Wahyuni et al. (2023), penipuan digital dalam pelayanan publik dapat terjadi dalam berbagai bentuk, seperti phishing, pencurian identitas, hingga penggunaan data palsu untuk mengakses layanan tertentu. Penelitian ini menekankan bahwa penipuan digital tidak hanya merugikan individu tetapi juga dapat mengganggu kepercayaan publik terhadap institusi pemerintah.

Meningkatnya kasus penipuan digital menunjukkan bahwa sebagian masyarakat masih memiliki keterbatasan dalam literasi digital, khususnya dalam mengenali modus kejahatan siber dan melindungi data pribadi di ruang digital (Baltezarević, 2022). Kondisi ini menyebabkan individu rentan terhadap manipulasi informasi, tautan berbahaya, serta penyalahgunaan identitas digital. Oleh karena itu, pendampingan literasi digital menjadi upaya preventif yang penting untuk meningkatkan pemahaman masyarakat tentang risiko penipuan digital sekaligus membekali mereka dengan keterampilan praktis dalam mengidentifikasi dan menghindari berbagai bentuk kejahatan siber (Hidayat et al., 2024; Rullah et al., 2025).

Kegiatan pengabdian masyarakat ini didasari oleh meningkatnya kasus penipuan digital, terutama di kalangan masyarakat yang kurang memahami risiko dan cara melindungi diri di dunia maya (Amelia, 2023). Minimnya kesadaran dan pengetahuan tentang keamanan digital menjadi salah satu faktor utama yang membuat masyarakat rentan terhadap penipuan. Oleh karena itu, kegiatan ini bertujuan untuk memberikan edukasi mengenai bahaya penipuan digital dan bagaimana cara menghadapinya (Fauzi et al., 2023).

Dalam kajian literatur, Yundari et al. (2024) menemukan bahwa sektor pelayanan publik menjadi target utama bagi para pelaku penipuan digital karena sering kali data pribadi masyarakat tersimpan dalam sistem digital yang dikelola oleh pemerintah. Ketika data ini disalahgunakan, potensi kerugian yang ditimbulkan dapat sangat besar. Beberapa kasus penipuan digital dalam pelayanan publik, seperti pencurian data kesehatan dan data

administrasi kependudukan, menunjukkan bahwa tingkat kesadaran masyarakat dan institusi terkait mengenai perlindungan data masih perlu ditingkatkan.

Kajian dari Jayanti et al. (2024) menunjukkan bahwa penggunaan teknologi digital dalam pelayanan publik memang memberikan kemudahan, namun juga memiliki risiko keamanan yang signifikan. Penelitian ini merekomendasikan pentingnya penerapan langkah-langkah pengamanan yang lebih ketat, termasuk edukasi kepada masyarakat tentang cara mengenali ciri-ciri penipuan digital, penguatan sistem keamanan data, serta perlunya kolaborasi antara pemerintah dan penyedia layanan teknologi dalam menangkal ancaman penipuan. Temuan penelitian terbaru juga memperkuat pentingnya literasi digital sebagai strategi pencegahan penipuan di ruang digital. Studi Li et al. (2024) menunjukkan bahwa tingkat literasi digital yang lebih tinggi berkontribusi signifikan dalam menurunkan risiko masyarakat menjadi korban penipuan daring, terutama melalui peningkatan kemampuan dalam mengenali pola penipuan dan mengambil keputusan yang lebih aman saat berinteraksi secara digital. Selain itu, penelitian Zulfa & Najicha (2022) menegaskan bahwa edukasi dan pendampingan literasi digital yang terstruktur mampu meningkatkan kesadaran masyarakat terhadap berbagai modus penipuan (*scam awareness*) serta mendorong perilaku preventif dalam penggunaan media digital. Kedua penelitian tersebut menegaskan bahwa pendekatan edukatif berbasis pendampingan merupakan instrumen efektif dalam memperkuat ketahanan masyarakat terhadap ancaman penipuan digital.

Tingginya tingkat penetrasi internet di Indonesia, yang mencapai lebih dari 210 juta pengguna pada tahun 2023 Ningsih & Rahyuni (2023), turut meningkatkan risiko masyarakat terhadap ancaman penipuan digital. Fenomena ini diperburuk dengan masih rendahnya literasi digital di kalangan masyarakat, khususnya dalam mengenali modus penipuan berbasis teknologi. Banyak individu, terutama yang tidak memiliki latar belakang teknologi informasi, masih kesulitan membedakan antara informasi asli dan palsu, maupun tautan berbahaya yang tersebar melalui pesan singkat, email, atau media sosial. Hal ini menunjukkan adanya kebutuhan mendesak untuk memberikan edukasi yang tepat sasaran agar masyarakat dapat menjadi lebih waspada dan tangguh terhadap serangan siber yang semakin kompleks.

Tujuan utama kegiatan pengabdian masyarakat ini adalah untuk meningkatkan kesadaran masyarakat tentang berbagai bentuk penipuan digital yang sering terjadi. Selain itu, kegiatan ini juga bertujuan untuk memberikan keterampilan praktis kepada masyarakat agar dapat melindungi diri dan data pribadi mereka dari berbagai ancaman di dunia maya. Manfaat dari kegiatan ini diharapkan mampu menciptakan komunitas yang lebih tanggap terhadap bahaya penipuan digital, serta mampu mengambil langkah preventif yang tepat untuk menjaga keamanan

data pribadi mereka. Melalui edukasi yang berkelanjutan, masyarakat diharapkan menjadi lebih mandiri dalam menghadapi ancaman digital dan mengurangi risiko menjadi korban penipuan di masa depan.

## B. METODE PELAKSANAAN

Metode pelaksanaan kegiatan pengabdian masyarakat ini dilakukan melalui webinar “Ngobrol Bareng Legislator” dengan tema “Waspada Penipuan Digital di Dunia Maya” yang diselenggarakan oleh Kementerian Komunikasi dan Informatika Republik Indonesia bekerja sama dengan Komisi I DPR RI. Kegiatan ini melibatkan 120 peserta dari masyarakat umum yang mengikuti webinar secara daring. Mitra kegiatan berperan dalam mendukung perencanaan, fasilitasi teknis, serta koordinasi pelaksanaan kegiatan agar tujuan edukasi dapat tercapai secara optimal.

Tahap pra-pelaksanaan meliputi penyusunan materi edukasi terkait penipuan digital, penentuan alur kegiatan, serta koordinasi teknis dengan mitra pelaksana. Seluruh pelaksanaan webinar difasilitasi oleh rekanan yang ditunjuk oleh Kominfo, yaitu Intel Studio yang berlokasi di Pasar Minggu, Jakarta Selatan, termasuk pengelolaan teknis acara, pengaturan platform daring, serta komunikasi dengan narasumber, moderator, dan peserta. Tahap pelaksanaan dilakukan secara daring melalui platform *Zoom* dan disiarkan secara langsung melalui kanal YouTube Intel Studio, sehingga memungkinkan jangkauan peserta yang lebih luas (Prasetya & Surbakti, 2023).

Tahap evaluasi dilakukan setelah seluruh rangkaian webinar selesai untuk menilai efektivitas kegiatan dalam meningkatkan pemahaman peserta mengenai berbagai bentuk penipuan digital di dunia maya. Tahap evaluasi dilakukan dengan menggunakan metode *pre-test* dan *post-test*. *Pre-test* diberikan kepada peserta sebelum kegiatan webinar dimulai untuk mengidentifikasi tingkat pengetahuan awal mengenai jenis-jenis penipuan digital, ciri-ciri penipuan, serta langkah pencegahan yang dapat dilakukan. Setelah seluruh rangkaian materi dan diskusi selesai, peserta diberikan *post-test* dengan instrumen pertanyaan yang serupa untuk menilai perubahan tingkat pemahaman dan kesadaran peserta. Hasil perbandingan antara *pre-test* dan *post-test* menunjukkan adanya peningkatan signifikan pada pemahaman peserta, yang tercermin dari kemampuan peserta dalam mengenali modus penipuan digital dan menerapkan langkah-langkah preventif dalam penggunaan media digital.

## C. HASIL DAN PEMBAHASAN

Pada tahap persiapan, kegiatan pengabdian masyarakat difokuskan pada penyusunan materi edukasi yang relevan dengan kebutuhan masyarakat terkait penipuan digital di dunia maya. Materi disusun untuk memberikan pemahaman dasar mengenai jenis-jenis penipuan digital yang

umum terjadi serta langkah-langkah pencegahannya. Persiapan ini bertujuan agar materi yang disampaikan mudah dipahami oleh peserta dengan latar belakang literasi digital yang beragam, sekaligus sesuai dengan tujuan kegiatan pendampingan literasi digital.

Pada tahap pelaksanaan, kegiatan pengabdian masyarakat diwujudkan melalui webinar Ngobrol Bareng Legislator dengan tema “Waspada Penipuan Digital di Dunia Maya” yang dilaksanakan secara daring melalui platform Zoom dan diikuti oleh peserta dari Jakarta Pusat, Jakarta Selatan, serta luar negeri (Gambar 1 dan 2). Dalam kegiatan ini, penulis berperan sebagai salah satu narasumber yang menyampaikan materi mengenai penipuan digital di dunia maya. Selain melalui Zoom, kegiatan ini juga disiarkan secara langsung melalui kanal YouTube Intel Studio. Rekaman acara webinar ini dapat dilihat melalui tautan *youtube* berikut ini: [https://www.youtube.com/watch?v=JQep9\\_23L78&t=6885s](https://www.youtube.com/watch?v=JQep9_23L78&t=6885s). Materi yang disampaikan mencakup berbagai bentuk penipuan *online*, seperti *phishing*, *pharming*, *sniffing*, *money mule*, serta serangan *social engineering* yang bertujuan memperoleh informasi sensitif atau mendorong korban melakukan transfer dana secara tidak sadar (Azzani et al., 2023; Mahesa et al., 2023), seperti terlihat pada Gambar 1 dan Gambar 2.



**Gambar 1.** Narasumber Menyampaikan Materi Keamanan Siber



**Gambar 2.** Peserta Menyampaikan Pertanyaan

Pembahasan lebih lanjut menekankan bahwa *phishing* merupakan salah satu ancaman utama, di mana pelaku menggunakan identitas palsu dengan meniru institusi atau individu tepercaya untuk memperoleh data sensitif, seperti kata sandi, PIN, dan informasi kartu kredit. Ciri umum penipuan ini antara lain penggunaan bahasa yang bersifat mendesak dan sapaan umum kepada calon korban (Hartono, 2023). Untuk mencegah risiko tersebut,

peserta diberikan pemahaman mengenai langkah-langkah pengamanan, seperti penggunaan kata sandi yang kuat, aktivasi autentikasi dua faktor, pemanfaatan perangkat lunak antivirus, serta kewaspadaan terhadap tautan dan tawaran yang mencurigakan (Altuk, 2021). Selain itu, dijelaskan pula prosedur yang dapat dilakukan apabila seseorang menjadi korban penipuan digital, yaitu dengan segera melaporkan kejadian kepada pihak berwenang disertai bukti pendukung yang relevan (Suryati et al., 2024).

Terkait kewaspadaan umum ditekankan pentingnya untuk bersikap skeptis terhadap telepon atau pesan tak dikenal yang menawarkan hadiah. Pengguna diharapkan untuk mengenali jenis-jenis penipuan digital dan melaporkan aktivitas mencurigakan, terutama jika telah membagikan informasi sensitif seperti kode OTP (Nurdiansyah et al., 2023). Narasumber menekankan pentingnya melakukan pengamanan perangkat digital, termasuk menggunakan otentikasi sidik jari dan wajah, serta memperbarui antivirus secara rutin. Pengguna juga disarankan untuk memilih perangkat dari agen resmi dan selalu memeriksa kesesuaian kode perangkat dengan kemasan (Permadi & Rokhman, 2023).

Tahap evaluasi dilakukan menggunakan metode *pre-test* dan *post-test* untuk mengukur tingkat peningkatan pemahaman peserta terhadap penipuan digital setelah mengikuti kegiatan pendampingan. Instrumen evaluasi terdiri dari 10 butir soal pilihan ganda yang sama pada *pre-test* dan *post-test*. Soal-soal tersebut disusun berdasarkan empat indikator capaian, yaitu: (1) pemahaman jenis-jenis penipuan digital, (2) kemampuan mengenali ciri dan modus penipuan, (3) pemahaman langkah pencegahan penipuan digital, serta (4) pengetahuan mengenai tindakan yang harus dilakukan apabila menjadi korban penipuan digital. *Pre-test* diberikan sebelum pemaparan materi untuk mengidentifikasi tingkat pengetahuan awal peserta, sedangkan *post-test* diberikan setelah seluruh rangkaian materi dan diskusi selesai untuk mengukur perubahan pemahaman.

Hasil evaluasi menunjukkan adanya peningkatan yang signifikan pada pemahaman peserta setelah kegiatan pendampingan. Secara keseluruhan, skor rata-rata pemahaman peserta meningkat dari kategori sedang pada *pre-test* menjadi kategori tinggi pada *post-test*. Peningkatan paling menonjol terlihat pada indikator kemampuan mengenali modus penipuan dan langkah pencegahan, yang menunjukkan bahwa materi pendampingan yang disampaikan melalui webinar efektif dalam meningkatkan kesadaran dan kewaspadaan peserta terhadap penipuan digital di dunia maya. Tingkat pemahaman peserta terhadap materi pendampingan secara keseluruhan meningkat hingga 75%, yang menegaskan keberhasilan kegiatan pengabdian masyarakat ini dalam meningkatkan literasi digital masyarakat. Rincian hasil evaluasi disajikan pada Tabel 1 berikut.

**Tabel 1.** Peningkatan Pemahaman dan Keterampilan Peserta

Indikator Pemahaman	Rata-rata <i>Pre-test (%)</i>	Rata-rata <i>Post-test (%)</i>
Pemahaman jenis-jenis penipuan digital	42	88
Kemampuan mengenali modus penipuan digital	55	92
Pemahaman langkah pencegahan penipuan digital	38	90
Pengetahuan tindakan saat menjadi korban penipuan	40	85
Rata-rata keseluruhan	50	87

## D. SIMPULAN DAN SARAN

Simpulan kegiatan pengabdian kepada masyarakat mengenai kewaspadaan terhadap penipuan digital di dunia maya berhasil menjawab permasalahan terkait rendahnya kesadaran dan pemahaman masyarakat tentang bahaya penipuan di era digital. Dari hasil kegiatan, terjadi peningkatan signifikan sebesar 75 % dalam pengetahuan peserta mengenai jenis-jenis penipuan digital yang umum terjadi, strategi yang digunakan oleh pelaku penipuan, serta langkah-langkah yang dapat diambil untuk menghindari menjadi korban. Dampak dari kegiatan ini terlihat dari perubahan perilaku peserta yang mulai lebih berhati-hati dalam berinteraksi di dunia maya, seperti menghindari mengklik tautan yang mencurigakan, memverifikasi keaslian sumber informasi, dan menggunakan metode otentifikasi dua faktor untuk melindungi akun daring mereka.

Untuk kegiatan selanjutnya, disarankan agar program edukasi tentang kewaspadaan penipuan digital di dunia maya dilakukan dengan cakupan yang lebih luas dan melibatkan lebih banyak komunitas, termasuk kelompok rentan seperti orang tua dan pelajar. Kegiatan dapat ditingkatkan dengan menambahkan simulasi langsung mengenai cara mengenali ciri-ciri penipuan digital melalui workshop interaktif. Selain itu, kerjasama dengan lembaga pemerintah, dunia usaha, dan pakar keamanan siber dapat membantu menyediakan panduan yang lebih terperinci dan kasus nyata yang relevan bagi masyarakat.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Kementerian Komunikasi dan Informatika dan Komisi 1 DPR RI yang berkenan mengundang penulis sebagai narasumber.

## DAFTAR RUJUKAN

- Altuk, E. V. (2021). Detection and prevention of fraud in the digital era. *Machine Learning Applications for Accounting Disclosure and Fraud Detection*, 126-137.
- Amelia, A. (2023). Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online. *Jurnal Inovasi Global*, 1(1), 14-25.
- Azzani, I. K., Purwantoro, S. A., & Almubaroq, H. Z. (2023). Urgensi Peningkatan Kesadaran Masyarakat Tentang Kasus Penipuan Online Berkedok Kerja

- Paruh Waktu Sebagai Ancaman Negara. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 10(7), 3556-3568.
- Baltezarević, R. V. (2022). Digital literacy as a means of preventing cybercrime. *Baština*(57), 131-139.
- Fauzi, A. M. m., Wahyuni, A. T., Chintia, G., Nenci, I. S., Nurwahidah, N., & Sari, P. N. (2023). Edukasi Pencegahan Penipuan Online Berbasis Sosial Media di Desa Mekarwangi. *Jurnal Pengabdian Kepada Masyarakat*, 3(2), 60-73.
- Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains dan Teknologi*, 2(02), 55-62.
- Hendrik S, A. (2019). Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring. *Mimbar Hukum*, 31(1), 59-74.
- Hidayat, F., Syaheza, M. F. A., & Fauzi, F. (2024). Literasi digital, membekali anak dengan kemampuan digital. *Jurnal Pendekar Nusantara*, 1(3), 1-7.
- Jayanti, N. W. D. B., Sjamsuddin, S., & Saleh, C. (2024). Transformasi Digital: Program Inovasi Bali Smart Island dalam Peningkatan Kualitas Pelayanan Publik di Bali. *Jurnal Ilmiah Administrasi Publik*, 10(1), 93-108.
- Li, P., Li, Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. *International Review of Economics & Finance*, 91(3), 364-377.
- Mahesa, D., Hariyanti, P., & Hosnah, A. U. (2023). Implementasi Hukum Terhadap Pelaku Kejahatan Tindak Pidana Penipuan Online. *Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, 27), 53-62.
- Ningsih, V. R., & Rahyuni, V. S. (2023). Analisis penggunaan smartphone dan stres dengan kejadian insomnia pada mahasiswa kesehatan masyarakat universitas jambi. *Jurnal Kesmas Jambi*, 7(1), 49-54.
- Nurdiansyah, D., Anindira, Y. D., Muhibin, S. S., & Putri, A. H. (2023). Sosialisasi Digital Security Dalam Meningkatkan Edukasi Bermedia Digital Di Lingkungan Masyarakat Depok Baru. *Karunia: Jurnal Hasil Pengabdian Masyarakat Indonesia*, 2(1), 109-120.
- Permadi, I. B., & Rokhman, A. (2023). Implementasi Identitas Kependudukan Digital Dalam Upaya Pengamanan Data Pribadi. *JOPPAS: Journal of Public Policy and Administration Silampari*, 4(2), 80-88.
- Permatasari, P., Darmawan, D. H., Maharani, A. A., Sastie, N. A., Zumaris, I., Nugroho, R. A., Baha'udin, M. A., Nariswari, J. R., Nugroho, M. H. A., & Fauzia, L. F. (2024). Sosialisasi Pencegahan Penipuan Online: Upaya Edukasi Untuk Keamanan Masyarakat. *Media Pengabdian Kepada Masyarakat (MPKM)*, 3(01), 241-246.
- Prasetya, W., & Surbakti, F. P. (2023). Pelaksanaan Kegiatan Pengabdian Masyarakat Webinar Nasional Building Bright Future for Generation Z bagi Siswa-Siswi SMA Jabodetabek. *Jurnal Pengabdian Masyarakat Charitas*, 3(02), 45-52.
- Rullah, A. D., Silva, F. R., Pratama, E. T. H., & Purwanto, E. (2025). Strategi Komunikasi untuk Meningkatkan Literasi Digital di Kalangan Pemuda. *Jurnal Pemberdayaan Ekonomi dan Masyarakat*, 2(1), 16-16.
- Surbakti, F. P. S. (2024). Edukasi Tantangan Transformasi Digital di Dunia Bisnis pada Masyarakat Dapil Sumatera Selatan 2. *Jurnal Abdimas Ekonomi dan Bisnis*, 4(2), 175-182.
- Suryati, S., Sardana, L., Disurya, R., & Putra, Y. S. (2024). Penguatan Literasi Digital Dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law). *Wajah Hukum*, 8(1), 84-94.
- Wahyuni, W., Adytia, P., Fahmi, M., & Yunita, Y. (2023). Penguatan Literasi Digital Staff Pelayanan Publik di Kelurahan Sempaja Timur untuk Percepatan Transformasi Digital Sebagai Kota Penyangga IKN. *Lumbung Inovasi: Jurnal Pengabdian kepada Masyarakat*, 8(4), 943-963.

- Yundari, N. P., Fadhlurrahman, M. A., & Ma'arif, N. (2024). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, 7(1), 23-43.
- Zulfa, A., & Najicha, F. U. (2022). Urgensi Penguatan Identitas Nasional dalam Menghadapi Society 5.0 di Era Globalisasi. *Jurnal Kalacakra*, 3(2), 65-71.