



Peningkatan Pemahaman Literasi Hukum Digital untuk Mencegah Penipuan Online di Kelurahan Padangsari

Zaenal Arifin, Soegianto Soegianto, Syafran Sofyan,

Evi Evi, Dyah Ayu Rizka Wulandari, Ayu Wanofika

Magister Hukum, Universitas Semarang, Semarang, Indonesia

zaenal@usm.ac.id

Abstract

Online fraud is increasingly difficult to recognize because digital transactions, social media communication, and financial services expose users to phishing, impersonation, fraudulent offers, and requests for sensitive account information. The community service activity in Padangsari Urban Village aimed to strengthen residents' digital legal literacy so they could recognize online fraud, protect personal data, verify digital information, and understand preventive and legal responses. The activity used an educational and participatory approach through legal socialization, interactive discussion, case-oriented explanation, and pre-test and post-test evaluation. The evaluation covered five indicators: understanding of digital legal literacy, recognition of online fraud modes, personal data protection, information and transaction verification, and preventive or post-incident action. The report records an average "Know" response of 43% before the intervention and 86% after the intervention, an increase of 43 percentage points. The result indicates a substantial short-term gain in measured understanding. However, the evidence should not be interpreted as proof of sustained behavioral change or reduced fraud incidence because the available evaluation does not provide respondent-level data, item-level results, a comparison group, or follow-up measurement. The activity therefore demonstrates immediate educational effectiveness while also highlighting the need for repeated, practice-based, and behavior-oriented digital legal literacy programs.

Keywords: *Digital Legal Literacy; Online Fraud; Personal Data Protection; Phishing; Two-Factor Authentication*

Abstrak

Penipuan online semakin sulit dikenali karena penggunaan transaksi digital, media sosial, dan layanan keuangan membuka ruang bagi phishing, penyamaran identitas, tawaran palsu, serta permintaan data keamanan akun. Kegiatan pengabdian kepada masyarakat di Kelurahan Padangsari bertujuan meningkatkan literasi hukum digital agar warga mampu mengenali modus penipuan, melindungi data pribadi, melakukan verifikasi informasi, serta memahami langkah pencegahan dan tindakan setelah menjadi korban. Kegiatan menggunakan pendekatan edukatif dan partisipatif melalui sosialisasi hukum, diskusi interaktif, penjelasan berbasis kasus, serta evaluasi pre-test dan post-test. Instrumen evaluasi mencakup lima indikator, yaitu pemahaman literasi hukum digital, pengenalan modus penipuan online, perlindungan data pribadi, verifikasi informasi dan transaksi, serta langkah pencegahan atau tindakan setelah kejadian. Laporan mencatat rata-rata jawaban "Tahu" sebesar 43% sebelum kegiatan dan 86% sesudah kegiatan. Perubahan tersebut setara dengan peningkatan 43 poin persentase. Hasil menunjukkan kenaikan pemahaman jangka pendek yang kuat. Temuan tersebut belum cukup untuk membuktikan perubahan perilaku yang menetap atau penurunan kejadian penipuan karena data yang tersedia tidak memuat data responden, hasil per butir, kelompok pembandingan, maupun pengukuran lanjutan. Kegiatan ini menunjukkan efektivitas edukatif awal sekaligus menegaskan kebutuhan program literasi hukum digital yang berulang, berbasis praktik, dan berorientasi pada perubahan perilaku.

Kata kunci: Literasi Hukum Digital; Penipuan Online; Perlindungan Data Pribadi; Phishing; Verifikasi Dua Langkah



1. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah pola komunikasi, transaksi, dan akses layanan publik. Warga Kelurahan Padangsari, Kecamatan Banyumanik, Kota Semarang, menggunakan media sosial, belanja daring, dan layanan perbankan digital dalam aktivitas sehari-hari. Intensitas tersebut memperluas manfaat teknologi sekaligus memperbesar paparan terhadap penipuan online. Modus yang disebut dalam laporan meliputi *phishing*, investasi fiktif, jual beli daring fiktif, penyalahgunaan data, peretasan akun, serta penipuan yang mengatasnamakan lembaga tertentu. Risiko tidak berhenti pada kerugian materi. Korban dapat kehilangan kendali atas akun, data pribadi, dan kepercayaan terhadap transaksi digital (Sahara & Kuswandi, 2025). Laporan PKM menempatkan rendahnya literasi hukum digital sebagai persoalan utama karena sebagian warga belum memahami hak, kewajiban, serta risiko hukum yang melekat pada aktivitas digital.

Literasi hukum digital dalam kegiatan ini dipahami lebih luas daripada kemampuan menggunakan perangkat. Warga perlu mampu menilai informasi, mengenali tindakan yang berisiko, menjaga data pribadi, memahami konsekuensi hukum, dan memilih respons yang tepat (Purnama et al., 2021). Penguatan literasi digital ditempatkan sebagai bagian dari pencegahan pelanggaran hukum siber (Suryati et al., 2024). Pentingnya pemahaman UU ITE dalam aktivitas media *online* (Siregar et al., 2024). Literasi digital berbasis hukum perlu diarahkan pada kemampuan praktis masyarakat (Lobubun et al., 2024).

Penipuan digital memiliki karakter adaptif. Pelaku memanfaatkan situasi yang dianggap mendesak, rasa percaya, ketidaktelitian, dan kebiasaan pengguna dalam membuka tautan atau memberikan data. *Phishing* sebagai bentuk penipuan digital yang mengeksploitasi tautan dan kredensial pengguna (Akdemir & Yenal, 2021). Mekanisme penipuan digital dapat berkembang mengikuti pola aktivitas masyarakat (Utomo et al., 2024). Temuan tersebut menguatkan kebutuhan edukasi yang tidak berhenti pada pengenalan definisi, tetapi menghubungkan norma hukum dengan keputusan praktis.

Dasar hukum yang disampaikan dalam kegiatan meliputi UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. UU Nomor 19 Tahun 2016, KUHP Pasal 378 tentang penipuan, UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, dan UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Penyampaian regulasi tersebut penting untuk menjembatani jarak antara norma hukum dan perilaku pengguna. Perlindungan hukum tidak efektif jika warga hanya mengetahui nama peraturan tanpa mampu mengenali risiko, mengamankan akun, memverifikasi informasi, dan menempuh langkah setelah insiden (Nisa et al., 2023).

Kegiatan pengabdian ini diarahkan pada dua persoalan: kesenjangan pemahaman literasi hukum digital dan meningkatnya variasi modus penipuan online. Solusi yang digunakan berupa sosialisasi aplikatif, diskusi interaktif, pengenalan kasus, serta penekanan pada perlindungan data pribadi, verifikasi informasi, penggunaan verifikasi dua langkah (2FA), dan respons ketika



menjadi korban. Tujuan kegiatan adalah meningkatkan pemahaman warga Kelurahan Padangsari mengenai hukum digital dan membangun kemampuan preventif menghadapi penipuan online.

2. METODE

Kegiatan dilaksanakan di Kelurahan Padangsari, Kecamatan Banyumanik, Kota Semarang dengan sasaran unsur pemerintah kelurahan, LPMK, RT/RW, PKK, tokoh masyarakat, dan Karang Taruna. Pelaksanaan menggunakan pendekatan edukatif dan partisipatif. Kegiatan dimulai dengan pembukaan dan identifikasi pemahaman awal melalui *pre-test*. Materi kemudian disampaikan secara komunikatif dengan fokus pada literasi hukum digital, dasar hukum perlindungan di ruang digital, modus penipuan online, *phishing*, perlindungan data pribadi, verifikasi informasi, keamanan akun, 2FA, serta langkah pencegahan dan pelaporan. Sesi pemaparan dilanjutkan diskusi interaktif agar peserta dapat menghubungkan materi dengan pengalaman sehari-hari, termasuk pesan WhatsApp yang mengatasnamakan lembaga, tawaran hadiah yang tidak masuk akal, permintaan OTP, dan transaksi jual beli online yang merugikan. Evaluasi dilakukan menggunakan instrumen yang sama pada *pre-test* dan *post-test*. Laporan menyatakan terdapat lima pertanyaan utama dengan indikator literasi hukum digital, pengenalan modus penipuan online, perlindungan data pribadi, serta langkah pencegahan dan tindakan ketika menjadi korban. Data dianalisis secara deskriptif dengan membandingkan persentase rata-rata peserta yang menjawab “Tahu” sebelum dan sesudah kegiatan. Karena lampiran asli hanya menampilkan nomor 1–5 tanpa redaksi pertanyaan, lima pertanyaan pada Tabel 1 dirumuskan kembali berdasarkan indikator yang dijelaskan dalam laporan. Rumusan tersebut tidak diposisikan sebagai salinan redaksi instrumen asli.

Tabel 1. Rekonstruksi Indikator dan Pertanyaan Evaluasi

No.	Indikator	Pertanyaan
1	Literasi hukum digital	Apakah Anda memahami pengertian dan prinsip dasar literasi hukum digital dalam penggunaan internet?
2	Pengenalan modus penipuan	Apakah Anda dapat mengenali ciri penipuan online, termasuk phishing serta tautan atau situs palsu?
3	Perlindungan data pribadi	Apakah Anda memahami data pribadi dan data keamanan akun yang tidak boleh diberikan kepada pihak lain, termasuk PIN dan OTP?
4	Verifikasi informasi dan transaksi	Apakah Anda dapat melakukan verifikasi terhadap informasi, tautan, situs, atau aplikasi sebelum melakukan transaksi digital?
5	Pencegahan dan tindakan	Apakah Anda mengetahui langkah pencegahan dan tindakan yang tepat apabila mengalami atau menemukan penipuan online, termasuk penggunaan 2FA dan pelaporan?



Sumber: Diolah dari indikator evaluasi dalam laporan akhir PKM; redaksi pertanyaan merupakan rekonstruksi untuk kebutuhan artikel.

3. HASIL DAN PEMBAHASAN

Kegiatan memperoleh dukungan dari pemerintah kelurahan dan unsur masyarakat. Peserta berasal dari LPMK, RT/RW, PKK, tokoh masyarakat, Karang Taruna, serta unsur pemerintah kelurahan. Komposisi tersebut relevan dengan strategi pencegahan berbasis komunitas karena kelompok sasaran memiliki posisi penting dalam penyebaran informasi di tingkat lingkungan. Laporan mencatat respons peserta yang aktif pada sesi diskusi. Pertanyaan yang muncul berkaitan dengan pesan WhatsApp yang mengatasmakan lembaga, hadiah tidak masuk akal, permintaan OTP, dan transaksi daring yang merugikan (Wulandari et al., 2022). Materi menjadi lebih kontekstual karena dikaitkan dengan pengalaman yang dekat dengan aktivitas warga.



Gambar 1. Pelaksanaan Sosialisasi Literasi Hukum Digital

Penyampaian materi tidak berhenti pada pengenalan regulasi. Peserta diarahkan memahami hubungan antara norma hukum dan tindakan pencegahan. UU ITE, KUHP Pasal 378, UU Perlindungan Konsumen, dan UU Pelindungan Data Pribadi diperkenalkan sebagai kerangka perlindungan. Kerangka tersebut kemudian diterjemahkan ke dalam tindakan yang dapat dilakukan warga: tidak membagikan data pribadi, tidak memberikan OTP, memeriksa keaslian situs atau aplikasi, menghindari tautan mencurigakan, menggunakan platform pembayaran resmi, dan mengaktifkan 2FA (Balakrishnan et al., 2025). Pendekatan ini lebih operasional dibanding penyuluhan yang hanya berorientasi pada pengetahuan normatif.



Gambar 2. Penyampaian Materi oleh Narasumber

2FA menjadi salah satu contoh penghubung antara literasi hukum dan keamanan teknis (Effendy & Oktiani, 2024). Laporan menempatkan 2FA sebagai lapisan perlindungan tambahan yang dapat memperkecil peluang pengambilalihan akun ketika kata sandi diketahui pihak lain (Jubur et al., 2025). Selain itu sosialisasi ini juga membahas peningkatan keamanan melalui *two-step verification*. Namun, edukasi 2FA perlu dipahami secara proporsional. Fitur tersebut tidak menghilangkan seluruh risiko karena keamanan tetap bergantung pada kerahasiaan kode, perangkat, dan kewaspadaan pengguna. Karena itu, 2FA seharusnya ditempatkan sebagai bagian dari strategi berlapis, bukan satu-satunya solusi (Naqvi et al., 2023).

Kekuatan utama program terletak pada relevansi materi. Risiko digital dijelaskan melalui situasi konkret. Peserta tidak hanya diberi konsep *phishing*, tetapi juga diarahkan memeriksa tautan, menjaga OTP, memverifikasi platform, dan mengaktifkan 2FA. Strategi tersebut membuat literasi hukum tidak terpisah dari literasi keamanan digital (Auton & Sturman, 2025). Model ini penting karena penipuan online sering memanfaatkan keputusan pengguna dalam hitungan detik. Pengetahuan hukum yang tidak diterjemahkan menjadi keputusan praktis akan memiliki nilai pencegahan yang terbatas (Sturman et al., 2024). Program di Kelurahan Padangsari menerjemahkan pengetahuan tersebut melalui pengenalan situasi yang dekat dengan aktivitas masyarakat. Peserta diarahkan mengenali pesan WhatsApp yang mengatasnamakan lembaga, tawaran hadiah yang tidak masuk akal, permintaan OTP, transaksi jual beli daring yang merugikan, serta tautan yang mengarah pada situs mencurigakan (Wahyuddin et al., 2024).

Pengenalan modus diarahkan pada pembentukan pola pengambilan keputusan yang lebih hati-hati. Peserta tidak hanya dituntut mengenali indikasi penipuan, tetapi juga memahami kapan suatu komunikasi perlu dihentikan dan diperiksa kembali. Respons spontan terhadap pesan yang mendesak dapat meningkatkan risiko kesalahan keputusan. Karena itu, verifikasi ditempatkan sebagai mekanisme penyaring sebelum pengguna melanjutkan transaksi atau memberikan informasi keamanan. Pola ini menempatkan kewaspadaan sebagai proses pengambilan keputusan, bukan sekadar kemampuan mengenali istilah atau bentuk kejahatan siber (Nur'aini &



Simanjuntak, 2025).

Pengamanan akun menjadi bagian lanjutan dari strategi tersebut. Verifikasi dua langkah atau *two-factor authentication* (2FA) diperkenalkan sebagai lapisan keamanan tambahan ketika kata sandi tidak lagi menjadi satu-satunya perlindungan akun. Peserta memperoleh pemahaman bahwa kode verifikasi, perangkat, dan data keamanan harus dijaga secara bersamaan. Penerapan 2FA memperlihatkan bahwa perlindungan hukum di ruang digital membutuhkan dukungan perilaku keamanan yang konkret. Fitur tersebut tetap bukan perlindungan mutlak. Keamanan bergantung pada kerahasiaan kredensial dan kewaspadaan pengguna (Qadriah et al., 2023).

Pendekatan partisipatif memperkuat proses pembelajaran karena peserta dapat menghubungkan materi dengan pengalaman di lingkungan masing-masing. Keterlibatan LPMK, RT/RW, PKK, tokoh masyarakat, Karang Taruna, dan unsur pemerintah kelurahan juga membuka peluang penyebaran pengetahuan melalui jaringan sosial yang telah terbentuk. Pengetahuan mengenai pencegahan penipuan tidak berhenti pada peserta kegiatan, tetapi berpotensi diteruskan kepada keluarga dan kelompok masyarakat di tingkat lingkungan. Dengan demikian, kegiatan memiliki nilai preventif pada dua tingkat yakni meningkatkan kewaspadaan individu dan memperkuat kapasitas komunitas dalam merespons risiko digital.

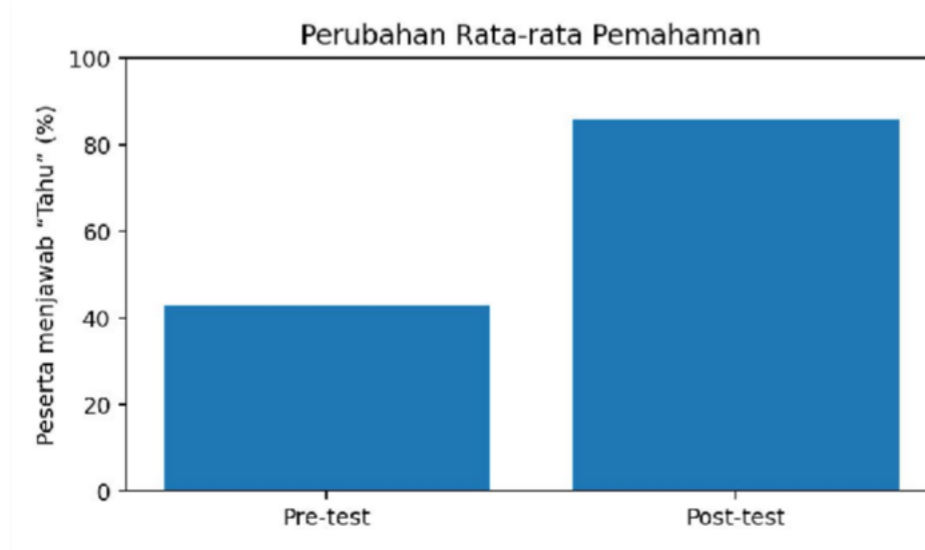
Rangkaian materi membentuk alur pencegahan yang sederhana: mengenali modus, menghentikan respons spontan, memeriksa sumber informasi, menjaga data keamanan akun, memastikan keaslian platform, menggunakan pengamanan tambahan, memilih kanal transaksi resmi, melaporkan kejadian. Alur tersebut membuat literasi hukum digital lebih dekat dengan kebutuhan masyarakat. Hukum hadir sebagai dasar pengambilan tindakan, bukan sekadar pengetahuan mengenai peraturan.

Laporan akhir mencatat rata-rata peserta yang menjawab “Tahu” sebesar 43% pada *pre-test* dan 86% pada *post-test*. Jawaban “Tidak Tahu” berubah dari 57% menjadi 14%. Perubahan rata-rata tersebut menunjukkan peningkatan sebesar 43 poin persentase. Angka 86% merupakan tingkat pemahaman setelah kegiatan, bukan besaran peningkatan. Koreksi interpretasi ini penting agar hasil tidak dibaca secara keliru sebagai kenaikan 86%.

Tabel 2. Perbandingan Hasil *Pre-Test* dan *Post-Test*

Indikator agregat	<i>Pre-test</i>	<i>Post-test</i>	Perubahan
Menjawab “Tahu”	43%	86%	+43 poin persentase
Menjawab “Tidak Tahu”	57%	14%	−43 poin persentase

Sumber: Laporan akhir PKM Kelurahan Padangsari; perhitungan perubahan oleh penulis.



Gambar 3. Perubahan rata-rata pemahaman peserta

Secara substantif, perubahan 43 poin persentase menunjukkan bahwa intervensi mampu meningkatkan jawaban pengetahuan pada saat evaluasi. Penurunan kategori “Tidak Tahu” dari 57% menjadi 14% memperlihatkan hasil yang konsisten. Temuan tersebut memperkuat posisi program sebagai bentuk edukasi hukum yang mengutamakan keterhubungan antara regulasi, risiko digital, serta tindakan pencegahan. Warga tidak hanya diperkenalkan pada istilah hukum. Warga dibekali pola mengenali penipuan, menjaga informasi keamanan akun, melakukan verifikasi, memperkuat keamanan akun, memilih tindakan ketika menghadapi risiko digital. Pola pembelajaran tersebut relevan dengan kondisi masyarakat Padangsari yang menggunakan media sosial, belanja daring, layanan perbankan digital, serta berbagai layanan berbasis internet dalam aktivitas sehari-hari.

4. PENUTUP

Kegiatan pengabdian kepada masyarakat di Kelurahan Padangsari menunjukkan hasil positif dalam meningkatkan pemahaman literasi hukum digital untuk pencegahan penipuan online. Materi menghubungkan dasar hukum dengan risiko yang dihadapi warga, seperti *phishing*, penyalahgunaan data, permintaan OTP, transaksi palsu, dan pengambilalihan akun. Pendekatan sosialisasi dan diskusi interaktif memberi ruang bagi peserta untuk mengaitkan materi dengan pengalaman sehari-hari. Evaluasi menunjukkan rata-rata jawaban “Tahu” meningkat dari 43% pada *pre-test* menjadi 86% pada *post-test*. Perubahan tersebut sebesar 43 poin persentase. Hasil ini menunjukkan efektivitas edukasi dalam meningkatkan pemahaman jangka pendek. Temuan belum dapat dipakai untuk menyatakan adanya perubahan perilaku jangka panjang, penurunan korban, atau penurunan kejadian penipuan. Keterbatasan berasal dari data agregat, ketiadaan hasil per butir, jumlah responden, kelompok pembanding, dan pengukuran lanjutan. Program berikutnya perlu menggunakan evaluasi yang lebih kuat melalui pertanyaan terstandar, pencatatan hasil per indikator, simulasi kasus, pengukuran perilaku, dan *post-test* tertunda. Edukasi berkala melalui struktur kelurahan juga perlu dikembangkan agar



pengetahuan berubah menjadi kebiasaan keamanan digital yang konsisten.

UCAPAN TERIMA KASIH

Tim mengucapkan terima kasih kepada Universitas Semarang melalui LPPM, Pascasarjana, Program Studi Magister Hukum, Kelurahan Padangsari, serta unsur LPMK, RT/RW, PKK, tokoh masyarakat, dan Karang Taruna yang mendukung pelaksanaan kegiatan. Kegiatan ini dibiayai oleh Universitas Semarang sesuai Perjanjian Pelaksanaan Kegiatan Pengabdian kepada Masyarakat Nomor 084/USM.H7.LPPM/N/2025.

DAFTAR PUSTAKA

- Akdemir, N., & Yenil, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *SAGE Open*, 11(3), 1–19. <https://doi.org/10.1177/21582440211031879>
- Auton, J. C., & Sturman, D. (2025). Persuasion under pressure: the influence of persuasion principles and time constraints on phishing email susceptibility. *Information and Computer Security*, 33(5), 845–859. <https://doi.org/10.1108/ICS-07-2024-0163>
- Balakrishnan, V., Ahmmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLOS ONE*, 20(1), e0317232. <https://doi.org/10.1371/journal.pone.0317232>
- Effendy, M. Y., & Oktiani, H. (2024). Literasi Digital Keamanan Siber pada Remaja menghadapi Social Engineering. *Wacana Publik*, 18(1), 35–42. <https://doi.org/10.37295/wp.v18i1.67>
- Jubur, M., Shrestha, P., & Saxena, N. (2025). An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools. *ACM Computing Surveys*, 57(5), 1–32. <https://doi.org/10.1145/3711117>
- Lobubun, M., Sari, R. I. R., & Rifaldi, A. (2024). Mencerdaskan Kehidupan Masyarakat Pesisir: Pendampingan Literasi Digital Berbasis Hukum sebagai Implementasi Pasal 31 UUD 1945 di Biak Timur. *Legal Empowerment: Jurnal Pengabdian Hukum*, 2(2), 76–86. <https://doi.org/10.46924/legalempowerment.v2i2.278>
- Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyediji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132, 103387. <https://doi.org/10.1016/j.cose.2023.103387>
- Nisa, U., Nisak, C. L. C., & Fatia, D. (2023). Literasi Digital Lansia Pada Aspek Digital Skill dan Digital Safety. *Jurnal Komunikasi Global*, 12(1), 143–167. <https://doi.org/10.24815/jkg.v12i1.31667>
- Nur'aini, R. J., & Simanjuntak, M. (2025). PHISHING AWARENESS AND SECURITY CONCERNS: ANALYZING THE ROLE OF ANTI-PHISHING KNOWLEDGE AND INTERNET EXPERIENCE IN ONLINE BANKING USERS. *Jurnal Ilmu Keluarga Dan Konsumen*, 18(2), 121–133. <https://doi.org/10.24156/jikk.2025.18.2.121>
- Purnama, S., Ulfah, M., Machali, I., Wibowo, A., & Narmaditya, B. S. (2021). Does digital literacy influence students' online risk? Evidence from Covid-19. *Heliyon*, 7(6), e07406. <https://doi.org/10.1016/j.heliyon.2021.e07406>
- Qadriah, L., Achmady, S., & Husaini. (2023). Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentication (2FA). *Jurnal*



- Sains Dan Informatika*, 9(1), 29–35. <https://doi.org/10.34128/jsi.v9i1.519>
- Sahara, A., & Kuswandi. (2025). Penipuan Online sebagai Bentuk Kejahatan Siber dalam Perspektif Kriminologi. *Parlementer: Jurnal Studi Hukum Dan Administrasi Publik*, 2(4), 93–105. <https://doi.org/10.62383/parlementer.v2i4.1425>
- Siregar, D., Adlina, M., Salsabilla, P. C., Sitepu, K., Halawa, A. A., Gulo, A. E., Ndraha, A., Halawa, H., & Halawa, Y. (2024). Penyuluhan Hukum; Penggunaan literasi digital sebagai upaya penanggulangan berita hoax dan bijak bermedia sosial bagi pelajar di kota Medan. *BEMAS: Jurnal Bermasyarakat*, 5(1), 6–14. <https://doi.org/10.37373/bemas.v5i1.999>
- Sturman, D., Bell, E. A., Auton, J. C., Breakey, G. R., & Wiggins, M. W. (2024). The roles of phishing knowledge, cue utilization, and decision styles in phishing email detection. *Applied Ergonomics*, 119, 1–11. <https://doi.org/10.1016/j.apergo.2024.104309>
- 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. <https://doi.org/10.33087/wjh.v8i1.1447>
- Utomo, F. W., Mauludin Insana, D. R., & Mayndarto, E. C. (2024). Mekanisme Penipuan Digital pada Masyarakat Era 5.0 (Studi Kasus Penipuan Online Berbasis Lowongan Kerja Paruh Waktu yang Merebak di Masyarakat). *Jurnal Ilmiah WUNY*, 6(1), 32–41. <https://doi.org/10.21831/jwuny.v6i1.72257>
- Wahyuddin, Ersal, L. F., Aningsih, G., Hidayat, T., & Sonni, A. F. (2024). Analisis Jaringan Komunikasi Penipuan Online Melalui Media Sosial WhatsApp Messenger. *Jurnal Netnografi Komunikasi*, 2(2), 33–50. <https://doi.org/10.59408/jnk.v2i2.27>
- Wulandari, N., Adnan, M. S., & Wicaksono, C. B. (2022). Are You a Soft Target for Cyber Attack? Drivers of Susceptibility to Social Engineering-Based Cyber Attack (SECA): A Case Study of Mobile Messaging Application. *Human Behavior and Emerging Technologies*, 2022(1), 5738969. <https://doi.org/10.1155/2022/5738969>

Ucapan Terimakasih

Para penulis menyampaikan terima kasih yang tulus kepada Editor dan Reviewer anonim atas waktu yang telah diberikan, komentar yang berwawasan, serta saran konstruktif yang secara signifikan telah berkontribusi terhadap penyempurnaan artikel ini. Para penulis juga berharap bahwa artikel ini dapat memberikan wawasan yang bermanfaat dan memberikan kontribusi yang berarti terhadap perkembangan diskusi di bidang terkait, serta dapat memberikan manfaat bagi para pembaca dan peneliti di masa mendatang.

Informasi Pendanaan

Penelitian ini didanai secara mandiri oleh penulis.

Pernyataan Benturan Kepentingan

Para penulis menyatakan bahwa **tidak terdapat benturan kepentingan** dalam publikasi artikel ini.

Pernyataan Etika Publikasi dan Orisinalitas

Para penulis menegaskan bahwa penelitian ini merupakan karya yang sepenuhnya orisinal. Naskah ini belum pernah dipublikasikan, baik dalam bentuk cetak, daring, maupun media lainnya, serta tidak sedang diajukan ke jurnal lain untuk proses penelaahan. Seluruh sumber yang dicantumkan dalam daftar pustaka telah ditulis sesuai dengan kaidah dan etika sitasi akademik yang berlaku.

**Pernyataan Penggunaan Kecerdasan Buatan Generatif**

Para penulis menyatakan bahwa kecerdasan buatan generatif digunakan sebagai alat bantu dalam proses penyusunan manuskrip ini. Secara khusus, ChatGPT dan Grammarly digunakan untuk meningkatkan kualitas bahasa dan keterbacaan teks secara keseluruhan.

Seluruh keluaran yang dihasilkan oleh kecerdasan buatan kemudian ditinjau secara kritis, disunting, dan diverifikasi oleh para penulis untuk memastikan keakuratan serta menjaga integritas ilmiah. Para penulis bertanggung jawab sepenuhnya atas isi akhir manuskrip.

Penggunaan kecerdasan buatan generatif dibatasi hanya pada fungsi pendukung dan tidak dianggap sebagai bentuk kepenulisan. Selain itu, tidak terdapat analisis maupun interpretasi data yang dilakukan oleh kecerdasan buatan tanpa pengawasan dan keterlibatan aktif dari penulis.