Journal of Community Service, Empowerment Studies and Sustainable Solution
https://ejournal.natacendekia.org/index.php/JoCEPASS
Vol. 1, No. 3, Juli 2026, Hal. 220-228
e-ISSN 3125-0041

PENINGKATAN LITERASI KEAMANAN SIBER DAN PERLINDUNGAN DATA DIGITAL BAGI MASYARAKAT DESA KLAMBIR LIMA KEBUN

Rizky Rahmansyah[1*], Sumarno[2], Mohammad Yusup [3], Rivaldo Siburian [4]
[1]Program Studi Teknik Informatika, Universitas Prima Indonesia, Indonesia
[2]Program Studi Ilmu Hukum, Universitas Pembangunan Panca Budi, Indonesia
[3]Program Studi Sains Data, Universitas Pembangunan Panca Budi, Indonesia
[4]Program Studi Teknik Informatika, Universitas Prima Indonesia, Indonesia
rizkyrahmansyah@unprimdn.ac.id, sumarno@dosen.pancabudi.ac.id, yusuf@dosen.pancabudi.ac.id, rivaldosiburian2906@gmail.com

ARTICLE INFO

Article History:

Received : 15/07/2026
Revised : 29/07/2026
Accepted : 30/07/2026
Online : 31/07/2026

Kata Kunci:
Literasi Digital,
Keamanan Siber,
Perlindungan Data,
Masyarakat Desa,
Pengabdian Masyarakat

Keywords:
Digital Literacy,
Cyber Security,
Data Protection,
Rural Community,
Community Service

ABSTRACT

Abstrak: Perkembangan teknologi digital mendorong masyarakat desa semakin aktif menggunakan telepon pintar, media sosial, aplikasi pesan, dan layanan daring, tetapi pemanfaatan tersebut belum selalu diikuti pemahaman yang memadai tentang keamanan data pribadi. Mitra sasaran kegiatan adalah Pemerintah Desa Klambir Lima Kebun dengan peserta sebanyak 16 orang yang terdiri atas perangkat desa, pelaku usaha kecil, pemuda, dan masyarakat umum. Kegiatan ini bertujuan meningkatkan pemahaman peserta mengenai ancaman siber, perlindungan data pribadi, penggunaan kata sandi yang aman, verifikasi dua langkah, serta pengenalan pesan dan tautan mencurigakan. Pelaksanaan menggunakan pendekatan edukatif dan partisipatif melalui sosialisasi interaktif, ceramah singkat, diskusi, tanya jawab, dan simulasi kasus. Evaluasi dilakukan secara formatif melalui pengamatan partisipasi, tanya jawab, diskusi reflektif, dan identifikasi contoh pesan penipuan. Hasil evaluasi menunjukkan bahwa peserta memahami pentingnya menjaga kerahasiaan data pribadi, tidak membagikan kode OTP, menggunakan kata sandi yang kuat dan berbeda, mengaktifkan pengamanan tambahan, serta memverifikasi pesan sebelum membuka tautan atau memberikan informasi. Kegiatan ini menunjukkan bahwa edukasi berbasis contoh nyata dan bahasa sederhana relevan untuk membangun kebiasaan digital yang lebih aman pada masyarakat non-teknis, meskipun perubahan perilaku jangka panjang masih memerlukan pendampingan dan evaluasi lanjutan.

Abstract: The growing use of digital technology has encouraged rural communities to rely more on smartphones, social media, messaging applications, and online services; however, this use is not always accompanied by adequate knowledge of personal data security. The target partner was the Government of Klambir Lima Kebun Village, involving 16 participants consisting of village officials, small-business actors, youth, and community members. This community service activity aimed to improve participants' understanding of cyber threats, personal data protection, secure password practices, two-step verification, and the identification of suspicious messages and links.

The activity employed an educational and participatory approach through interactive outreach, short lectures, discussions, question-and-answer sessions, and case simulations. Formative evaluation was conducted through observation of participation, reflective discussion, questions, and exercises to identify fraudulent messages. The evaluation indicated that participants understood the importance of protecting personal data, never sharing one-time passwords, using strong and different passwords, enabling additional account protection, and verifying messages before opening links or disclosing information. These findings suggest that education using real-life examples and accessible language is relevant for developing safer digital habits among non-technical communities, although long-term behavioral change requires further mentoring and evaluation.

Crossref

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

A. LATAR BELAKANG

Perkembangan teknologi digital telah mengubah pola komunikasi, transaksi, pembelajaran, dan akses layanan publik, termasuk pada masyarakat desa. Asosiasi Penyelenggara Jasa Internet Indonesia mencatat bahwa jumlah pengguna internet di Indonesia pada 2024 mencapai 221,56 juta jiwa dengan penetrasi 79,5% (Asosiasi Penyelenggara Jasa Internet Indonesia, 2024). Peningkatan tersebut menunjukkan bahwa penggunaan layanan digital telah menjadi bagian dari aktivitas sehari-hari masyarakat dan perlu diimbangi dengan kemampuan menggunakan teknologi secara aman (Siti Maesaroh, 2025).

Kemudahan digital juga menghadirkan risiko berupa penipuan daring, pencurian akun, phishing, malware, penyalahgunaan identitas, dan kebocoran data pribadi. Keamanan siber tidak hanya berhubungan dengan sistem dan jaringan, tetapi juga dengan kemampuan pengguna dalam memahami risiko, melindungi akun, mendeteksi pesan mencurigakan, merespons insiden, dan memulihkan akses setelah terjadi gangguan (National Institute of Standards and Technology, 2024). Praktik autentikasi yang baik, termasuk penggunaan kata sandi yang kuat dan autentikasi multifaktor, menjadi bagian penting dalam perlindungan akun digital (Temoshok et al., 2025).

Desa Klambir Lima Kebun berada di Kecamatan Hamparan Perak, Kabupaten Deli Serdang. Data tahun 2024 menunjukkan bahwa wilayah desa memiliki luas 24,02 km^2, berjarak sekitar 9 km dari ibu kota kecamatan dan 42 km dari ibu kota kabupaten, serta dihuni 23.356 jiwa. Jumlah tersebut merupakan populasi terbesar di antara desa/kelurahan di Kecamatan Hamparan Perak (Badan Pusat Statistik Kabupaten Deli Serdang, 2025). Luas wilayah dan besarnya jumlah penduduk memperlihatkan pentingnya penyebaran informasi yang mudah dijangkau, termasuk melalui telepon pintar, aplikasi pesan, media sosial, dan layanan daring (Ruslan et al., 2025).

Berdasarkan identifikasi awal tim bersama mitra, masyarakat telah menggunakan telepon pintar dan layanan digital untuk komunikasi, transaksi, promosi usaha, serta

pertukaran informasi. Namun, penggunaan tersebut belum selalu disertai pemahaman yang cukup mengenai tanda-tanda phishing, perlindungan kode OTP, keamanan kata sandi, pengaturan privasi, dan verifikasi identitas pengirim. Ancaman rekayasa sosial memanfaatkan kebiasaan, kepercayaan, konteks pesan, dan keterbatasan pengguna dalam menilai risiko sehingga edukasi perlu berfokus pada kemampuan mengenali serta merespons pesan mencurigakan (Albladi & Weir, 2018) (Das et al., 2019).

Data pribadi seperti NIK, nomor telepon, alamat, foto identitas, informasi rekening, kata sandi, dan kode OTP perlu dilindungi karena dapat disalahgunakan untuk pembajakan akun, penipuan, atau pencurian identitas (Siddiqi et al., 2022). Di Indonesia, Undang-Undang Nomor 27 Tahun 2022 mengatur hak subjek data pribadi, kewajiban pengendali dan prosesor data, larangan penyalahgunaan data, serta sanksi terhadap pelanggaran pelindungan data pribadi (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022). Pemahaman terhadap hak dan tanggung jawab tersebut perlu diterjemahkan ke dalam kebiasaan sederhana yang dapat diterapkan masyarakat sehari-hari (Hidayat & Anwar, 2024).

Literasi keamanan digital merupakan salah satu unsur penting dalam literasi digital, bersama kecakapan digital, etika digital, dan budaya digital (Kementerian Komunikasi dan Informatika Republik Indonesia & Katadata Insight Center, 2022). Rendahnya kewaspadaan terhadap tautan palsu, permintaan data yang tidak wajar, akun tiruan, dan pesan yang membangun rasa takut atau urgensi dapat meningkatkan kerentanan pengguna (Atriani et al., 2024). Oleh karena itu, masyarakat memerlukan pembelajaran yang kontekstual, tidak terlalu teknis, dan menggunakan contoh yang dekat dengan pengalaman mereka.

Program edukasi keamanan siber perlu menggabungkan penyampaian informasi dengan diskusi, praktik, simulasi, dan penguatan kebiasaan aman. Pemberian informasi saja belum selalu menghasilkan perubahan perilaku, sehingga materi perlu relevan, mudah dipahami, dan dilengkapi kesempatan untuk berlatih mengambil keputusan (Bada et al., 2019). Kegiatan serupa pada masyarakat desa juga menunjukkan bahwa ceramah interaktif, diskusi, praktik, serta evaluasi dapat membantu meningkatkan pemahaman mengenai phishing dan perlindungan data (Hamsar & Nasyuha, 2025)

Berdasarkan analisis situasi tersebut, kegiatan pengabdian ini bertujuan untuk: (1) meningkatkan pemahaman masyarakat mengenai ancaman siber dan jenis data pribadi yang perlu dilindungi; (2) melatih peserta mengenali pesan, akun, dan tautan mencurigakan melalui contoh kasus; serta (3) mendorong penerapan kebiasaan aman berupa penggunaan kata sandi yang kuat dan berbeda, pengaktifan verifikasi dua langkah, pengaturan privasi, verifikasi informasi, dan pelaporan indikasi penipuan. Kegiatan ini menjadi bentuk penerapan ilmu Teknik Informatika, khususnya keamanan informasi, melalui pendekatan edukatif yang sesuai bagi masyarakat non-teknis.

B. METODE PELAKSANAAN

Kegiatan pengabdian dilaksanakan di Desa Klambir Lima Kebun, Kecamatan Hamparan Perak, Kabupaten Deli Serdang, pada hari Jum'at, 26 Juni 2026. Mitra

kegiatan adalah Pemerintah Desa Klambir Lima Kebun. Peserta yang terlibat berjumlah 16 orang, terdiri atas perangkat desa, pelaku usaha kecil, pemuda, dan masyarakat umum yang menggunakan telepon pintar, media sosial, aplikasi pesan, serta layanan digital dalam kegiatan sehari-hari. Penetapan peserta dilakukan melalui koordinasi dengan perangkat desa agar kelompok sasaran sesuai dengan kebutuhan program.

Metode pelaksanaan menggunakan pendekatan edukatif dan partisipatif dalam bentuk sosialisasi, ceramah singkat, diskusi, tanya jawab, praktik, dan simulasi kasus. Pendekatan edukatif digunakan untuk membangun pemahaman dasar mengenai keamanan siber dan perlindungan data, sedangkan pendekatan partisipatif memberi ruang kepada peserta untuk menyampaikan pengalaman, mengajukan pertanyaan, serta mempraktikkan cara mengenali ancaman digital. Materi disampaikan dengan bahasa sederhana dan contoh yang dekat dengan penggunaan WhatsApp, media sosial, layanan keuangan digital, dan akun daring.



Gambar 1. Pemaparan Materi Oleh Tim PKM

Tahap persiapan meliputi koordinasi dengan pemerintah desa, identifikasi kebutuhan mitra, penentuan sasaran peserta, penyusunan materi, pemilihan contoh kasus, serta penyiapan media presentasi dan instrumen evaluasi. Identifikasi kebutuhan difokuskan pada permasalahan yang sering dihadapi pengguna, yaitu pesan hadiah palsu, tautan tidak resmi, permintaan kode OTP, pembajakan akun, penggunaan kata sandi lemah, dan penyebaran data pribadi. Hasil tahap ini digunakan untuk menyesuaikan istilah, contoh, dan tingkat kedalaman materi dengan karakteristik peserta.

Tahap pelaksanaan dilakukan melalui sosialisasi dan pelatihan tatap muka. Materi meliputi pengertian keamanan siber, bentuk ancaman digital, perlindungan data pribadi, pembuatan kata sandi yang kuat dan berbeda, penggunaan verifikasi dua langkah, pengaturan privasi media sosial, keamanan perangkat, tindakan awal ketika akun bermasalah, serta prosedur penyimpanan bukti dan pelaporan kasus. Penyampaian materi diselingi diskusi dan tanya jawab agar peserta dapat menghubungkan konsep dengan pengalaman yang pernah ditemui.

Praktik dan simulasi dilakukan dengan menampilkan contoh pesan hadiah, permintaan OTP, tautan dengan alamat tidak wajar, akun yang meniru pihak tertentu, dan pesan yang menggunakan bahasa mendesak. Peserta diminta mengamati identitas

pengirim, isi pesan, alamat tautan, permintaan data, dan bentuk tekanan yang digunakan. Setelah itu, peserta mendiskusikan tindakan yang tepat, seperti tidak membuka tautan, tidak memberikan data, memverifikasi melalui kanal resmi, memblokir akun, mengganti kata sandi, dan menyimpan bukti digital.

Tahap evaluasi dilakukan secara formatif melalui pengamatan partisipasi, tanya jawab, diskusi reflektif, serta latihan mengidentifikasi contoh pesan dan tautan mencurigakan. Indikator evaluasi mencakup kemampuan peserta menjelaskan data yang harus dirahasiakan, mengenali tanda penipuan, menyebutkan ciri kata sandi yang aman, memahami fungsi verifikasi dua langkah, dan menentukan tindakan awal ketika menerima pesan mencurigakan. Hasil evaluasi dianalisis secara deskriptif berdasarkan jawaban peserta dan catatan pengamatan tim.



Gambar 2. Foto Bersama Masyarakat Desa Klambir Lima Kebun

Tindak lanjut diberikan dalam bentuk panduan praktis yang dapat diterapkan secara mandiri, yaitu menggunakan kata sandi yang berbeda untuk akun penting, mengaktifkan autentikasi tambahan, memperbarui perangkat lunak, memeriksa alamat tautan, tidak membagikan kode OTP, menyimpan tangkapan layar dan riwayat transaksi, serta melaporkan indikasi penipuan kepada platform, penyedia layanan keuangan, perangkat desa, atau pihak berwenang. Pemerintah desa juga didorong untuk menyebarkan pengingat keamanan digital melalui kanal komunikasi warga.

Metode tersebut dipilih karena sesuai dengan karakteristik peserta yang beragam dan berorientasi pada penerapan langsung. Evaluasi kegiatan belum menggunakan desain pre-test dan post-test terstandar sehingga hasil yang diperoleh bersifat deskriptif dan menggambarkan pemahaman peserta pada saat kegiatan. Pengukuran perubahan perilaku jangka panjang memerlukan pendampingan serta evaluasi lanjutan.

C. HASIL DAN PEMBAHASAN

1. Tahap Persiapan

Pada tahap persiapan, tim melakukan koordinasi dengan pemerintah desa untuk menetapkan waktu, tempat, sasaran, dan kebutuhan teknis kegiatan. Identifikasi awal menunjukkan bahwa topik yang paling relevan bagi peserta adalah penipuan melalui aplikasi pesan, permintaan kode OTP, tautan palsu, pembajakan akun, serta penyebaran foto identitas dan informasi rekening. Temuan tersebut digunakan untuk menyusun

materi berbasis kasus sehari-hari dan mengurangi penggunaan istilah teknis yang sulit dipahami. Tim juga menyiapkan media presentasi, contoh tangkapan layar pesan, lembar pertanyaan, dan panduan tindakan awal.

2. Tahap Pelaksanaan

Tabel 1. Materi Kegiatan

No.	Materi Kegiatan	Pokok Pembahasan	Tujuan Materi
1	Pengenalan Keamanan Siber	Pengertian keamanan siber, risiko penggunaan teknologi, dan tanggung jawab pengguna	Membangun pemahaman awal bahwa keamanan digital berkaitan dengan aktivitas sehari-hari
2	Ancaman Siber yang Sering Terjadi	Phishing, penipuan daring, tautan palsu, pencurian akun, malware, dan rekayasa sosial	Membantu peserta mengenali bentuk ancaman digital yang umum
3	Perlindungan Data Pribadi	NIK, nomor telepon, alamat, foto identitas, data rekening, kata sandi, PIN, dan kode OTP	Meningkatkan kesadaran agar data pribadi tidak dibagikan sembarangan
4	Kata Sandi yang Aman	Kata sandi panjang, kuat, berbeda untuk setiap akun, dan penggunaan pengelola kata sandi	Mendorong penggunaan kata sandi yang lebih aman
5	Verifikasi Dua Langkah	Fungsi autentikasi tambahan pada email, media sosial, aplikasi pesan, dan akun penting	Memberikan lapisan perlindungan tambahan pada akun
6	Keamanan Media Sosial dan Aplikasi Pesan	Pengaturan privasi, akun palsu, permintaan pertemanan, tautan, dan pesan mencurigakan	Meningkatkan kehati-hatian saat berinteraksi di platform digital
7	Simulasi Pesan Penipuan	Contoh hadiah palsu, permintaan OTP, tautan tidak resmi, akun tiruan, dan bahasa mendesak	Melatih peserta mengenali indikator penipuan melalui contoh nyata
8	Pencegahan, Penanganan, dan Pelaporan	Mengamankan akun, menyimpan bukti, menghubungi kanal resmi, dan melaporkan kasus	Membekali peserta dengan tindakan awal dan prosedur pelaporan yang tepat

Pelaksanaan kegiatan berlangsung pada hari Jum'at, 26 Juni 2026 dan diikuti oleh 16 peserta. Sosialisasi diawali dengan pemahaman bahwa keamanan siber berkaitan langsung dengan aktivitas sehari-hari, bukan hanya persoalan teknis. Materi kemudian disampaikan secara bertahap mulai dari pengenalan ancaman, perlindungan data pribadi, keamanan akun, hingga tindakan awal dan prosedur pelaporan. Susunan materi ditampilkan pada Tabel 1.

Diskusi menunjukkan bahwa contoh pesan yang mengatasnamakan bank, keluarga, kurir, atau penyelenggara hadiah paling mudah dipahami karena dekat dengan pengalaman peserta. Peserta diarahkan untuk tidak hanya menilai pesan dari nama atau foto profil, tetapi juga memeriksa konteks, alamat tautan, permintaan data, kesalahan penulisan, tekanan waktu, dan ketidakwajaran isi. Pembahasan ini sejalan dengan temuan bahwa rekayasa sosial memanfaatkan konteks dan karakteristik pengguna untuk memengaruhi penilaian terhadap pesan (Albladi & Weir, 2018).

Pada sesi perlindungan akun, peserta memperoleh panduan untuk membuat kata sandi yang panjang, kuat, dan berbeda pada setiap akun penting serta mengaktifkan verifikasi dua langkah. Peserta juga diingatkan agar tidak menyimpan atau mengirim kata sandi dan kode OTP melalui percakapan yang dapat diakses pihak lain. Praktik keamanan tersebut mendukung penggunaan autentikasi yang lebih kuat dan mengurangi ketergantungan pada satu faktor pengamanan (Rahmansyah & Meiditra,

2025). Simulasi kemudian melatih peserta untuk menghentikan respons spontan, memverifikasi pengirim melalui kanal resmi, dan menyimpan bukti apabila pesan diduga sebagai penipuan.



Gambar 3. Kegiatan PKM

3. Tahap Evaluasi dan Tindak Lanjut

Evaluasi formatif menunjukkan bahwa jawaban dan tanggapan peserta telah mencakup prinsip utama yang dilatihkan, yaitu menjaga kerahasiaan NIK, foto identitas, informasi rekening, kata sandi, PIN, dan kode OTP; mengenali pesan yang mendesak atau meminta data; serta melakukan verifikasi sebelum membuka tautan. Dalam latihan identifikasi, peserta dapat menjelaskan alasan suatu pesan perlu dicurigai dan menyebutkan tindakan yang lebih aman, seperti mengabaikan tautan, menghubungi pihak terkait melalui kontak resmi, memblokir akun, dan mengganti kata sandi apabila informasi telah terlanjur diberikan.

Hasil tersebut memperlihatkan bahwa penggunaan contoh nyata, diskusi, dan simulasi membantu peserta menghubungkan materi dengan situasi yang mungkin mereka hadapi. Temuan ini konsisten dengan kegiatan pengabdian di masyarakat desa yang menekankan efektivitas pembelajaran interaktif dan praktik langsung untuk memperkuat kesadaran keamanan data (Hamsar & Nasyuha, 2025; Ruslan et al., 2025). Setelah kegiatan, peserta menerima arahan mengenai pengamanan akun, penyimpanan bukti digital, dan jalur pelaporan. Namun, karena evaluasi belum menggunakan pre-test dan post-test terstandar, hasil ini terbatas pada capaian pemahaman saat kegiatan dan belum dapat digunakan untuk menyimpulkan perubahan perilaku jangka panjang.

D. SIMPULAN DAN SARAN

Kegiatan pengabdian mengenai literasi keamanan siber dan perlindungan data digital telah dilaksanakan melalui sosialisasi interaktif, diskusi, tanya jawab, dan simulasi kasus kepada masyarakat Desa Klambir Lima Kebun. Berdasarkan evaluasi formatif, peserta memahami jenis data yang perlu dirahasiakan, tanda umum pesan penipuan, pentingnya penggunaan kata sandi yang kuat dan berbeda, fungsi verifikasi dua langkah, serta tindakan aman sebelum membuka tautan atau memberikan

informasi. Dengan demikian, tujuan untuk meningkatkan pemahaman dasar dan kemampuan mengenali ancaman digital telah tercapai secara deskriptif.

Pendekatan berbasis contoh nyata dan bahasa sederhana membuat materi lebih mudah dikaitkan dengan pengalaman peserta. Meskipun demikian, evaluasi belum menggunakan pre-test dan post-test terstandar serta belum mengamati perubahan perilaku dalam jangka panjang. Oleh sebab itu, hasil kegiatan tidak ditafsirkan sebagai ukuran kuantitatif peningkatan literasi, melainkan sebagai gambaran pemahaman peserta selama proses pelatihan.

Kegiatan lanjutan disarankan menggunakan instrumen pre-test dan post-test, simulasi berkala, serta pendampingan pada kelompok yang berisiko tinggi, seperti pelaku UMKM, remaja, orang tua, dan pengelola layanan desa. Pemerintah desa dapat menyebarkan pengingat keamanan melalui grup komunikasi warga dan menetapkan kanal rujukan ketika masyarakat menerima pesan mencurigakan atau mengalami insiden. Program berkelanjutan diperlukan agar pengetahuan yang diperoleh berkembang menjadi kebiasaan digital yang aman.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Pemerintah Desa Klambir Lima Kebun yang telah memberikan izin, dukungan, dan fasilitas dalam pelaksanaan kegiatan pengabdian masyarakat ini. Ucapan terima kasih juga disampaikan kepada perangkat desa dan seluruh masyarakat Desa Klambir Lima Kebun yang telah berpartisipasi secara aktif dalam kegiatan sosialisasi dan pelatihan literasi keamanan siber serta perlindungan data digital.

Penulis juga menyampaikan terima kasih kepada pihak perguruan tinggi, tim pelaksana pengabdian, serta seluruh pihak yang telah membantu dalam proses persiapan, pelaksanaan, hingga penyusunan artikel ini. Dukungan dan kerja sama yang diberikan sangat membantu terlaksananya kegiatan pengabdian dengan baik, sehingga diharapkan hasil kegiatan ini dapat memberikan manfaat bagi masyarakat dalam meningkatkan kesadaran dan kebiasaan aman dalam menggunakan teknologi digital.

DAFTAR RUJUKAN

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*, 5. https://doi.org/10.1186/s13673-018-0128-7

Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). *Pengguna internet Indonesia tembus 221 juta orang*. Https://Apjii.or.Id/Berita/d/Apjii-Jumlah-Pengguna-Internet-Indonesia-Tembus-221-Juta-Orang. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Atriani, D., Purba, A., Sampetoding, E., & Husain, S. (2024). Transformation of Digital Literacy and Cyber Law in Rural Society: A Systematic Literature Review. *Proceedings of the 4th International Conference on Rural Socio-Economic Transformation, RUSET 2023, 1 November 2023, Bogor, Indonesia*. https://doi.org/10.4108/eai.1-11-2023.2344332

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv. https://doi.org/10.48550/arXiv.1901.02672

Das, S., Kim, A., Tingle, Z., & Nippert-Eng, C. (2019). *All about phishing: Exploring user research through a systematic literature review*. arXiv. https://doi.org/10.48550/arXiv.1908.05897

Hamsar, A., & Nasyuha, A. H. (2025). Digital literacy education to strengthen data security awareness in rural communities in Tobek Godang Village. *Jurnal IPTEK Bagi Masyarakat*, *5*(1), 128–135. https://doi.org/10.55537/j-ibm.v5i1.1306

Hidayat, R., & Anwar, N. (2024). Forensic analysis of web phishing and social engineering using the National Institute of Standards and Technology method: Case study of Facebook account data theft. *Journal of Digital Security and Forensics*, *1*(1). https://doi.org/10.29121/digisecforensics.v1.i1.2024.14

Kementerian Komunikasi dan Informatika Republik Indonesia & Katadata Insight Center. (2022). *Status literasi digital di Indonesia 2022*. Kementerian Komunikasi dan Informatika Republik Indonesia.

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Rahmansyah, R., & Meiditra, I. (2025). Network security system implementation using intrusion prevention system and honeypot technology at the Regional Revenue Office (Bapenda) of Padang City. *Internet of Things and Artificial Intelligence Journal*, *5*(3), 797–817. https://doi.org/10.31763/iota.v5i3.1013

Ruslan, A., Aris, V., Taufik, M., Hamzah, Q., & Asmirani, S. (2025). Pelatihan keamanan digital untuk meningkatkan cyber security awareness bagi masyarakat di Kelurahan Bontonompo Kabupaten Gowa. *LOSARI: Jurnal Pengabdian Kepada Masyarakat*, *7*(2), 206–214. https://doi.org/10.53860/losari.v7i2.509

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042. https://doi.org/10.3390/app12126042

Siti Maesaroh, R. (2025). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(2), 255–274. https://doi.org/10.14421/3n8bxw79

Temoshok, D., Choong, Y.-Y., Regenscheid, A., Galluzzo, R., Fenton, J. L., Richer, J., & Lefkovitz, N. (2025). *Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63B-4

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022).