Kacanegara Jurnal Pengabdian Pada Masyarakat
ISSN: 2615-6717 (Print)
ISSN: 2657-2338 (Online)
Terakreditasi Sinta 4 dari Kemenristekdikti No: 10/C/C3/DT.05.00/2025
DOI: 10.28989/kacanegara.v9i2.3528

Sosialisasi dan kampanye security awareness upaya pencegahan kejahatan siber di SPBU

Rama Sahtyawan[1*], Zennul Mubarrok[2], Yerly Ania Saputri[3], Muhammad Nasikh Afifuddin[4], Aditya Wahyu Ningrat[5], Rafi Adinata Rachmat[6]
[1,3,4,5,6]Program Studi Teknologi Informasi, FTTI, Universitas Jenderal Achmad Yani, Yogyakarta, Indonesia
[2]Program Studi Akuntansi, FES, Universitas Jenderal Achmad Yani, Yogyakarta, Indonesia

Article Info

Article history:

Received October 16, 2025
Accepted November 18, 2025
Published May 1, 2026

Kata Kunci:

Security Awareness;
Kejahatan Siber;
SPBU;
Pelatihan Keamanan Digital;
Skimming.

ABSTRAK

Program Pengabdian Kepada Masyarakat (PKM) ini berfokus pada upaya peningkatan *security awareness* untuk mencegah kejahatan siber di SPBU 44.555.05 Prujakan, Yogyakarta. Tujuannya adalah meningkatkan pemahaman pelanggan dan karyawan SPBU mengenai ancaman siber seperti *skimming*, *phishing*, dan *social engineering*, serta membangun budaya keamanan digital. Metode pelaksanaan mencakup sosialisasi, pelatihan, penerapan teknologi keamanan siber (seperti *firewall* dan antivirus), pendampingan, serta monitoring dan evaluasi. Hasilnya, program berhasil meningkatkan keterampilan dan kewaspadaan mitra terhadap ancaman siber, ditunjukkan dengan partisipasi aktif dan komitmen keberlanjutan. Disimpulkan bahwa pendekatan kolaboratif ini efektif dalam mengatasi permasalahan prioritas mitra dan mendukung implementasi MBKM. Saran yang diajukan adalah perlunya komitmen berkelanjutan dari mitra serta program replikasi untuk memperluas dampak positif ke SPBU lainnya.

Corresponding Author:
Rama Sahtyawan,
Prodi Teknologi Informasi,
Universitas Jenderal Achmad Yani Yogyakarta,
Jl. Siliwangi Jl. Ringroad Barat, Area Sawah, Banyuraden, Kec. Gamping, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55293
Email: *ramasahtyawan@gmail.com

1. PENDAHULUAN

Perkembangan teknologi digital telah mentransformasi berbagai sektor, termasuk sistem pembayaran di Stasiun Pengisian Bahan Bakar Umum (SPBU). Metode pembayaran non-tunai seperti kartu kredit/debit, QRIS, dan aplikasi MyPertamina semakin lazim digunakan karena kepraktisannya. Namun, di balik efisiensi yang ditawarkan, transisi digital ini diiringi oleh peningkatan ancaman kejahatan siber yang signifikan. SPBU sebagai titik transaksi yang padat dan strategis menjadi sasaran empuk bagi pelaku kejahatan, sehingga menciptakan lingkungan yang rentan bagi pelanggan dan operatornya[1].

Permasalahan utama yang dihadapi mitra SPBU 44.555.05 adalah Rendahnya tingkat kesadaran keamanan siber (*security awareness*) baik dari pihak pelanggan maupun petugas merupakan masalah utama yang juga ditemukan pada konteks UMKM dan ritel modern[2]. Banyak pelanggan yang tidak menyadari risiko seperti *skimming* pada mesin EDC, *phishing* melalui aplikasi palsu, atau manipulasi *social engineering*. Di sisi lain, operator SPBU juga belum mendapatkan pelatihan yang memadai untuk mengenali dan menangani ancaman tersebut[3,4]. Minimnya proteksi sistem dan tidak adanya prosedur standar penanganan insiden semakin memperparah kerentanan ini, mengakibatkan potensi kerugian finansial dan pencurian data[5].

Urgensi dari program ini terletak pada kebutuhan mendesak untuk membangun ketahanan siber di SPBU. Mengingat tingginya frekuensi dan nilai transaksi digital yang terjadi, tanpa upaya sistematis untuk meningkatkan kewaspadaan, pelanggan dan bisnis SPBU terus berada dalam ancaman yang dapat merusak kepercayaan dan stabilitas operasional[6,7]. Oleh karena itu, intervensi melalui pengabdian masyarakat menjadi krusial untuk memutus mata rantai eksploitasi kejahatan siber di lokasi yang vital ini[7,8].

Solusi yang ditawarkan dalam Program Kemitraan Masyarakat (PKM) ini tidak hanya terbatas pada sosialisasi konvensional, tetapi merupakan pendekatan komprehensif yang integratif. Program ini mengombinasikan edukasi melalui pelatihan dan kampanye, dengan penerapan teknologi keamanan siber sederhana seperti *firewall* dan antivirus, serta pendampingan berkelanjutan[10]. Pendekatan *blended* ini dirancang untuk menangani masalah dari hulu (pemahaman) hingga hilir (penerapan teknis)[11].

Inovasi pada PKM ini terletak pada penggabungan antara pendekatan edukasi partisipatif dengan sentuhan teknologi tepat guna, yang dikemas dalam sebuah program berkelanjutan[12]. Program ini juga secara eksplisit dirancang untuk mendukung kebijakan Merdeka Belajar Kampus Merdeka (MBKM), dimana mahasiswa terlibat langsung dalam proyek nyata di masyarakat[13]. Dengan demikian, PKM ini tidak hanya menjawab *gap* dari program sebelumnya yang mungkin masih bersifat insidental dan kurang mendalam, tetapi juga menciptakan dampak ganda: meningkatkan keamanan siber mitra sekaligus membekali mahasiswa dengan pengalaman belajar yang aplikatif[14].

2. METODE

Permasalahan yang muncul di SPBU 44.555.05 diantaranya Minimnya Pemahaman tentang Ancaman Siber**:** Baik pelanggan maupun petugas SPBU memiliki pengetahuan yang terbatas mengenai modus kejahatan siber kontemporer seperti *skimming* pada mesin EDC, *phishing* melalui tautan atau aplikasi palsu, dan teknik *social engineering* yang memanipulasi psikologis korban[15]. Kurangnya Prosedur Operasional Standar (POS): Tidak adanya panduan atau protokol yang jelas dan terbakukan untuk mendeteksi, melaporkan, dan menangani insiden keamanan siber. Petugas sering kali bingung harus bertindak apa ketika menemukan alat atau transaksi yang mencurigakan. Rendahnya Keterampilan Praktis: Operator dan karyawan SPBU belum memiliki keterampilan teknis dasar untuk mengoperasikan atau memelihara perangkat keamanan siber sederhana, seperti memastikan antivirus aktif atau mengenali indikasi *malware* pada sistem pembayaran[16]. Vulnerabilitas pada Sistem Digital: Sistem pembayaran digital yang digunakan rentan terhadap eksploitasi akibat kurangnya pembaruan (*update*) perangkat lunak secara berkala dan konfigurasi keamanan yang tidak optimal[17]. Serta Rendahnya tingkat kesadaran keamanan siber pada SPBU yang menunjukkan bahwa pelaku usaha ritel masih memiliki literasi siber yang terbatas, sehingga intervensi melalui pelatihan yang terstruktur sangat diperlukan[18]

Metode pelaksanaan kegiatan PKM di SPBU 44.555.05 Prujakan terdiri dari 5 tahapan meliputi Sosialisasi, persiapan, Profil peserta PKM, kegiatan Pelatihan, evaluasi.

1) Sosialisasi
   Pada tahap Sosialisasi, Tim PKM Memperkenalkan program PKM secara menyeluruh kepada semua pemangku kepentingan (pemilik, manajer, karyawan, dan perwakilan pelanggan) di SPBU untuk mendapatkan dukungan dan komitmen, Aktivitas yang dilakukan dengan melakukan pertemuan tatap muka untuk menjelaskan latar belakang, tujuan, manfaat, dan rangkaian kegiatan yang akan dilaksanakan. Forum ini juga digunakan untuk mengidentifikasi kebutuhan dan harapan spesifik mitra.
2) Persiapan
   Pada tahap Persiapan, bertujuan untuk menyiapkan semua materi, perangkat, dan infrastruktur pendukung yang diperlukan untuk memastikan kelancaran pelaksanaan. Pengembangan materi edukasi visual (poster, brosur, infografis) yang informatif dan mudah dipahami tentang berbagai jenis ancaman siber dan langkah pencegahannya, Penyusunan modul pelatihan yang mencakup teori dasar keamanan siber dan simulasi praktik, Penyiapan perangkat lunak keamanan (antivirus, *firewall* sederhana) dan penyusunan buku panduan pengoperasiannya, Koordinasi

 ISSN: 2615-6717 (Print), 2657-2338 (Online)

jadwal dan logistik dengan manajemen SPBU

3) Profil Peserta PKM.
   Program Pengabdian Kepada Masyarakat (PKM) ini melibatkan 15 orang peserta yang merupakan staf dari SPBU 44.555.05 Prujakan. Dari segi komposisi jenis kelamin, peserta terdiri dari 10 orang laki-laki (66,7%) dan 5 orang perempuan (33,3%). Rentang usia peserta berada pada kisaran 25 hingga 45 tahun, dengan mayoritas berada dalam kelompok usia produktif 30-40 tahun. Ditinjau dari latar belakang pendidikan, 80% peserta merupakan lulusan SMA atau SMK, sementara 20% sisanya memiliki latar belakang pendidikan Diploma Tiga (D3). Profil ini menunjukkan bahwa sebagian besar peserta merupakan tenaga operasional dengan dasar pendidikan menengah, sehingga pendekatan pelatihan lebih ditekankan pada aspek praktis dan aplikatif dengan penggunaan bahasa yang mudah dipahami.
4) Kegiatan Teknis Pelatihan
   Kegiatan pelatihan dilaksanakan secara intensif selama 8 jam, terbagi dalam dua sesi @ 4 jam, dengan pendekatan *blended learning* yang menggabungkan teori (40%) dan praktik (60%). Pelatihan melibatkan 15 orang peserta yang terdiri dari pengawas dan operator SPBU 44.555.05 Prujakan. Pemateri dalam kegiatan ini terdiri dari dosen Teknologi Informasi dan mahasiswa yang terlibat dalam program MBKM. Peran dosen sebagai fasilitator utama untuk materi teknis, sementara mahasiswa berperan sebagai pendamping dalam sesi praktik dan simulasi. Instrumen evaluasi yang digunakan berupa kuesioner *pretest* dan *posttest* yang terdiri dari 20 pertanyaan pilihan ganda mencakup tiga aspek: pengetahuan ancaman siber, deteksi *skimming*, dan penggunaan antivirus/*firewall*. Indikator keberhasilan pelatihan ditetapkan apabila minimal 80% peserta mencapai nilai posttest ≥70 dan mampu mendemonstrasikan instalasi serta konfigurasi dasar perangkat lunak keamanan siber.
5) Evaluasi
   Setelah kegiatan PKM selesai, dilakukan Evaluasi Program menjadi tahap krusial untuk mengukur keberhasilan dan dampak dari seluruh rangkaian kegiatan yang telah dilaksanakan. Evaluasi dilakukan melalui beberapa metode, dimulai dengan pembandingan hasil pretest dan posttest untuk mengukur peningkatan pengetahuan peserta secara kuantitatif. Selain itu, tim melakukan monitoring dan observasi langsung di lapangan untuk menilai penerapan praktik keamanan siber oleh karyawan pasca-pelatihan. Untuk mendapatkan umpan balik yang komprehensif, dilaksanakan juga forum diskusi partisipatif dengan manajemen dan staf SPBU.

3. HASIL DAN PEMBAHASAN

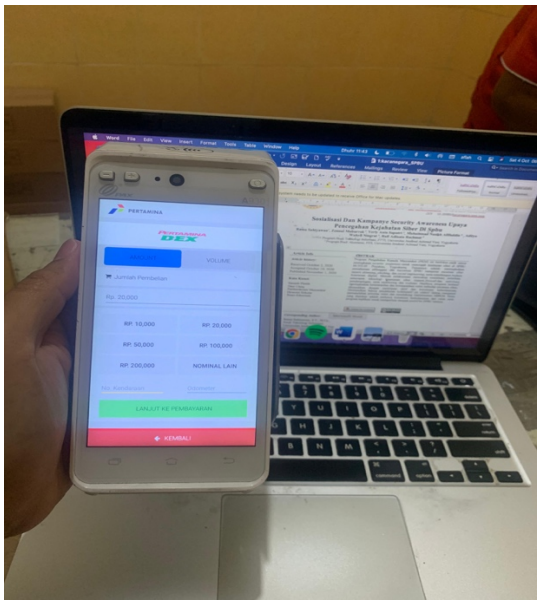
Pengabdian kepada masyarakat ini terdiri atas beberapa tahapan**,** Tahapan pertama pada hari kamis 27 agustus 2025 berupa Sosialisasi Tim PKM berkoordinasi dengan seluruh pemangku kepentingan SPBU, termasuk pemilik, manajer, karyawan, dan pelanggan. Hasilnya, tercapai pemahaman yang menyeluruh mengenai tujuan dan manfaat program PKM. Partisipasi aktif dari mitra terlihat dari antusiasme mereka dalam menyampaikan permasalahan yang sering dihadapi terkait keamanan siber. Sosialisasi ini berhasil menciptakan dasar yang kuat untuk tahapan selanjutnya, sekaligus membangun komitmen bersama dalam mengatasi ancaman kejahatan siber. Dokumentasi Sosialisasi pra kegiatan dapat dilihat pada Gambar 1.

Gambar 1. Sosialisasi pra kegiatan

Tahapan kedua adalah pelaksanaan kegiatan Pelatihan yang dilaksanakan pada hari kamis 4 september 2025 di SPBU prujakan mulai pukul 09:00. Acara dimulai dengan inspeksi diarea spbu mencakup pengenalan berbagai ancaman siber terkini seperti teknik phishing, social engineering. Foto area dispenser spbu dapat dilihat pada Gambar 2.

Tahapan ketiga pada tanggal 11 September 2025 yaitu pelatihan dilanjutkan dengan pemaparan singkat tentang keamanan siber pada mesin EDC untuk mengenali *skimming* palsu yang sering terjadi pada mesin EDC, Keamanan siber di mesin EDC SPBU penting untuk mencegah kejahatan skimming, yaitu pemasangan alat ilegal untuk mencuri data kartu. Pengelola SPBU dapat mengenali skimmer palsu dengan memeriksa tiga hal utama: fisik mesin (apakah card reader terasa longgar, warnanya tidak match, atau ada sisa lem), keypad (apakah terasa tebal tidak wajar atau responsnya lembek), dan lingkungan sekitar (apakah ada kamera mini tersembunyi), seperti Gambar 3.

Gambar 2. Foto area dispenser SPBU



Gambar 3. Mesin EDC

Pencegahan terbaik adalah dengan selalu menutupi PIN saat dimasukkan, memilih metode pembayaran yang lebih aman seperti tap atau QRIS, serta manajemen spbu harus memantau mutasi rekening secara rutin. Kewaspadaan sederhana ini sangat efektif melindungi dana SPBU dari risiko

 ISSN: 2615-6717 (Print), 2657-2338 (Online)

skimming. Tahapan Keempat pada tanggal 18 September 2025 yaitu pelatihan teknis dasar kepada pengawas SPBU untuk mengoperasikan atau memelihara perangkat keamanan siber sederhana, seperti mengenali indikasi *malware* pada sistem pembayaran. Pelatihan teknis dasar mengoperasikan keamanan siber dapat dilihat pada Gambar 4.

Gambar 4. Pelatihan teknis dasar mengoperasikan keamanan siber

Pelatihan ini mencakup cara memastikan perangkat lunak untuk mengenali tanda-tanda atau indikasi malware yang mencurigakan pada sistem pembayaran, seperti kinerja komputer yang tiba-tiba melambat atau munculnya notifikasi yang tidak biasa. Dengan demikian, pengawas dapat menjadi lini pertahanan pertama yang proaktif dalam menjaga integritas sistem transaksi di SPBU.

Pelatihan selanjutnya yaitu teknis dasar antivirus yang ditujukan khusus untuk para pengawas SPBU. Pelatihan ini difokuskan pada kemampuan praktis dalam mengoperasikannya. dan memelihara perangkat keamanan siber, dengan instruksi utama tentang cara memastikan software antivirus selalu aktif (running) dan terbarui (up-to-date) pada sistem pembayaran. pengawas SPBU dilatih untuk mengenali indikasi sederhana adanya malware, seperti kinerja komputer yang melambat tiba-tiba atau munculnya notifikasi mencurigakan, sehingga dapat mengambil tindakan awal yang tepat untuk mengamankan transaksi di SPBU prujakan. Pelatihan antivirus dapat dilihat pada Gambar 5.

Gambar 5. Pelatihan antivirus

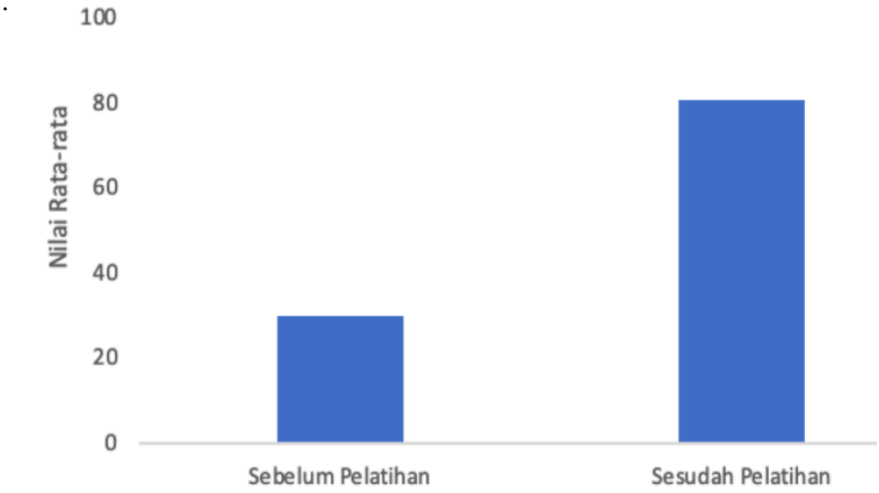
Pengawas SPBU dilatih untuk menjadi garis pertahanan pertama dengan mengenali indikasi sederhana adanya malware pada sistem komputer. Gejala utama yang harus diwaspadai tidak hanya mencakup kinerja komputer yang tiba-tiba menjadi sangat lambat atau sering hang, tetapi juga munculnya jendela pop-up (notifikasi) mencurigakan yang meminta data pribadi atau kata sandi, serta perubahan yang tidak dijelaskan pada setingan aplikasi atau munculnya program baru yang tidak dikenal.

Evaluasi efektivitas pelatihan dilakukan melalui metode *pretest* dan *posttest* untuk mengukur peningkatan pemahaman peserta. Hasilnya menunjukkan peningkatan yang signifikan, dimana nilai rata-rata *pretest* dan *posttest* sebagaimana Tabel 1 berikut.

Tabel 1. Hasil Evaluasi Pretest dan Posttest Pelatihan Security Awareness

No	Aspek yang Diukur	Rata-Rata Pretest	Rata-Rata Posttest	Peningkatan Nilai	Persentase Peningkatan	Standar Deviasi Pretest	Standar Deviasi Posttest
1	Pengetahuan Ancaman Siber (Phishing, Skimming)	32	82	+50	156.3%	8,5	5,2
2	Kemampuan Deteksi Skimming pada EDC	28	78	+50	178.6%	7,8	4,9
3	Pemahaman & Praktik Antivirus/Firewall	30	80	+50	166.7%	9,1	5,5
	Rata keseluruhan	30	80	+50	166.7%	8,5	5,2

Hal ini merepresentasikan peningkatan absolut sebesar 50 poin atau 166.7%. Data statistik lebih lanjut, seperti yang disajikan pada Tabel 1, mengonfirmasi bahwa peningkatan ini konsisten di semua aspek yang diukur, dengan standar deviasi yang mengecil, menunjukkan bahwa pemahaman peserta tidak hanya meningkat tetapi juga menjadi lebih merata setelah mengikuti pelatihan. Adapun Evaluasi sebelum dan setelah pelatihan ditunjukkan pada Gambar 6 berikut.



Gambar 6. Evaluasi sebelum dan setelah pelatihan

Peningkatan signifikan pada nilai posttest menyatakan bahwa pendekatan pelatihan partisipatif efektif dalam meningkatkan pemahaman teknis terhadap ancaman siber di SPBU[19]. Dampak dan implikasi dari Kegiatan PKM ini memberikan dampak positif yang signifikan dengan meningkatkan kesadaran dan pengetahuan karyawan serta pelanggan SPBU mengenai ancaman siber seperti *skimming*, *phishing*, dan *social engineering*. Hal ini dibarengi dengan peningkatan kapasitas teknis praktis para karyawan dalam mengoperasikan perangkat keamanan seperti antivirus dan *firewall*, serta kemampuan untuk mengenali indikasi *malware*. Melalui partisipasi aktif dan komitmen mitra, program ini tidak hanya memperkuat ketahanan siber SPBU mitra secara langsung tetapi juga menciptakan sebuah model yang dapat direplikasi untuk lokasi lain, sekaligus mendukung implementasi MBKM dengan melibatkan mahasiswa dalam penyelesaian masalah nyata,

 ISSN: 2615-6717 (Print), 2657-2338 (Online)

4. KESIMPULAN

Program Pengabdian Kepada Masyarakat (PKM) ini secara umum telah berhasil mencapai tujuannya untuk meningkatkan *security awareness* dan kapasitas teknis mitra SPBU 44.555.05 Prujakan dalam mencegah kejahatan siber. Keberhasilan ini tercermin dari capaian indikator kunci, yaitu peningkatan nilai rata-rata posttest sebesar 166.7%, serta kemampuan 100% peserta dalam mendemonstrasikan instalasi antivirus dan konfigurasi dasar *firewall*. Meskipun demikian, program ini memiliki keterbatasan, di antaranya durasi pelatihan yang relatif singkat dan belum mencakup seluruh karyawan SPBU. Untuk memastikan keberlanjutan program, disarankan agar diadakan pelatihan penyegaran setiap enam bulan sekali, dilakukan replikasi model serupa ke SPBU lain dalam jaringan yang sama, serta dibangun kolaborasi lebih lanjut dengan pihak perbankan atau penyedia layanan pembayaran digital untuk pelatihan keamanan transaksi EDC yang lebih mendalam.

DAFTAR PUSTAKA

[1] Puspita Kencana Sari, C. Candiwan, Nurvita Trianasari, and Adhi Prasetio, "Peningkatan Kesadaran Keamanan Siber Melalui Pelatihan Kepada Pelaku Umkm Binaan Yayasan Purba Danarta Semarang," Jurnal Pengabdian Kolaborasi dan Inovasi IPTEKS, vol. 3, no. 4, pp. 849-856, Aug. 2025, doi: 10.59407/jpki2.v3i4.2574

[2] S. Sahriyal, E. Erny, and N. Neswita, "Pelatihan Penggunaan Internet Bagi Pegawai Kantor dan Perangkat Desa Rantau Mapesai," Jurnal Pengabdian Masyarakat (abdira), vol. 2, no. 3, pp. 145-150, Jul. 2022, doi: 10.31004/abdira.v2i3.184

[3] S. Qomariyah, "Analisis Pengelolaan Pasar Tradisional Dan Sumber Daya Pedagang Terhadap Pendapatan Pedagang Pada Pasar Tradisional Boyolangu Kabupaten Tulungagung," Otonomi, vol. 22, no. 1, p. 12, Apr. 2022, doi: 10.32503/otonomi.v22i1.2396

[4] R. Nur Rohmah, "Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia," Cendekia Niaga, vol. 6, no. 1, pp. 1-11, Jul. 2022, doi: 10.52391/jcn.v6i1.629

[5] K. Waruwu et al., "Pendampingan Penyusunan Standar Operasional Prosedur Bagi Petugas Keamanan Di Rorinata Residence Suka Maju Kecamatan Sunggal Deliserdang," Mejuajua: Jurnal Pengabdian pada Masyarakat, vol. 1, no. 3, pp. 7-13, Apr. 2022, doi: 10.52622/mejuajuajabdimas.v1i3.27

[6] S. Alvi Sholikhatin, W. Fitrianingsih, and S. Dhiyaulhaq, "Workshop Strategi Peningkatan Popularitas Konten Serta Menjaga Keamanan Data Pribadi Di Berbagai Platform Media Sosial," SELAPARANG Jurnal Pengabdian Masyarakat Berkemajuan, vol. 4, no. 1, p. 251, Nov. 2020, doi: 10.31764/jpmb.v4i1.2929

[7] J. D. Laksono, L. Lindiasari, and H. Halimah, "Pengaruh Kampanye Pencegahan Kejahatan Melalui Spanduk Terhadap Penurunan Angka Kriminalitas," Brand Communication, vol. 4, no. 1, pp. 10-23, Jan. 2025, doi: 10.70704/bc.v4i1.360

[8] S. Sahriyal, E. Erny, and N. Neswita, "Pelatihan Penggunaan Internet Bagi Pegawai Kantor dan Perangkat Desa Rantau Mapesai," Jurnal Pengabdian Masyarakat (abdira), vol. 2, no. 3, pp. 145-150, Jul. 2022, doi: 10.31004/abdira.v2i3.184

[9] Moh. Wahib, B. Stafrezar, and A. Susanto, "Pembangunan Desa Berkelanjutan Melalui Partisipasi Masyarakat: Studi Kasus Pengabdian di Desa Catak Gayam," Jurnal Ekonomi, Pendidikan dan Pengabdian Masyarakat, vol. 1, no. 4, pp. 104-109, Nov. 2024, doi: 10.63200/jependimas.v1i4.33

[10] A. S. Ma'mun and G. Z. Muflih, "Implementasi Web Filtering Firewall Untuk Keamanan Pada Jaringan Internet Di Pondok Pesantren Al Hidayah Kebumen," SKANIKA: Sistem Komputer dan Teknik Informatika, vol. 8, no. 1, pp. 46-59, Jan. 2025, doi: 10.36080/skanika.v8i1.3298

[11] B. S. Putra and D. B. Santoso, "Analisis Keamanan Website Berbasis WordPress melalui Penetration Testing untuk Meningkatkan Keamanan Digital," Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi), vol. 9, no. 3, pp. 981-990, Jul. 2025, doi: 10.35870/jtik.v9i3.3692

[12] R. Ridwan and R. Ridwan, "Implementasi Program Poskestren Di Pondok Pesantren Nurul Iman Seberang Kota Jambi," Jurnal Promosi Kesehatan Poltekkes Bengkulu, vol. 2, no. 2, Jul. 2022, doi: 10.33088/jurnalprosehatkuu.v2i2.244

[13] Y. Adi Pratama, Dana Indra Sensuse, and Franky Juhar, "Identifikasi Tren Risiko Keamanan Siber dan Mitigasinya dalam Pembangunan Smart city," The Indonesian Journal of Computer Science, vol. 13, no. 6, Dec. 2024, doi: 10.33022/ijcs.v13i6.4524

[14] Baiq Dewi Lita Andiana and Muhammad Sayuti, "Pengaruh Digital Marketing Terhadap Peningkatan Penjualan UMKM," JOURNAL OF ECONOMIC, BUSINESS AND TOURISM, vol. 1, no. 3, Aug.

2025, doi: 10.70795/z5efnh42
[15] A. Ekaputra, S. Rachmalia, and N. Triyani, "Sosialisasi Pemanfaatan Aplikasi Pencatatan Keuangan Pada Ibu-Ibu PKK Di Perumnas Bojongbata Pemalang," Jurnal Entitas Pengabdian Masyarakat, vol. 1, no. 1, pp. 6-10, Jul. 2025, doi: 10.64465/jepm.v1i1.15
[16] T. Hastuti, Y. Djuyandi, and W. B. Darmawan, "Deteksi Dini Ancaman Social Engineering Hacker Terhadap Mata Pelajaran Rahasia Di Sekolah Staf Dan Komando Angkatan Udara," Paradigma POLISTAAT: Jurnal Ilmu Sosial dan Ilmu Politik, vol. 4, no. 1, pp. 60-81, Jun. 2021, doi: 10.23969/paradigmapolistaat.v4i1.4503
[17] J. Surya, A. Louis, A. Sopian, and F. H. Aminuddin, "Sistem Informasi Pengolahan Data Kelompok Usaha Bersama (SIKUBE) Pada Kantor Dinas Sosial Kota Jambi Berbasis Website," Jurnal Teknologi Informatika dan Komputer, vol. 8, no. 2, pp. 55-71, Sep. 2022, doi: 10.37012/jtik.v8i2.1209
[18] H. Santoso and I. Iwannudin, "Pendampingan Literasi Keuangan Digital pada Pelaku Usaha Mikro Kecil dan Menengan (UMKM) dalam Meningkatkan Manajemen Usaha," Jurnal Abdimas Berdaya : Jurnal Pembelajaran, Pemberdayaan dan Pengabdian Masyarakat, vol. 8, no. 2, p. 436, Sep. 2025, doi: 10.30736/jab.v8i2.1099
[19] M. Arisanty, Y. Riady, S. Anastassia Amellia Kharis, S. Maulidia Permatasari, and S. Sukatmi, "Cerdas Dan Aman Bermedia Digital : Peningkatan Kesadaran Keamanan Siber Di Era Hoaks Dan Phishing," Jurnal Pengabdian Kepada Masyarakat Patikala, vol. 4, no. 4, pp. 1407-1418, Jun. 2025, doi: 10.51574/patikala.v4i4.3282