

Penyuluhan Internet Sehat tentang Bahaya Phising dan Dampak Negatifnya bagi Siswa SMK N 4 Payakumbuh

Agus Nur Khomarudin¹, Romy Aulia², Jamaluddin³, Rina Novita⁴, Muhammad Ikhsan⁵,
Muhammad Naufal Afif⁶, Herdiansyah Suherlan⁷

^{1,7}Program Studi Teknologi Rekayasa Komputer, Politeknik Pertanian Negeri Payakumbuh

¹agusnurkhumarudin@gmail.com, ²romysinggalang@gmail.com,
³jamaluddin@politanipk.ac.id, ⁴rinanovita12345@gmail.com

Abstrak

Tindak kejahatan *phishing* adalah metode kejahatan siber (*cybercrime*) berupa *social engineering* di mana pelaku menyamar sebagai entitas terpercaya (bank, media sosial, lembaga pemerintah), untuk mencuri data sensitif seperti *username*, *password*, kartu kredit, dan data pribadi lainnya. Tindak kejahatan *phishing* dapat menimbulkan berbagai dampak meliputi: Dampak terhadap Data dan Akun Kehilangan akses akun & data pribadi, Dampak Finansial, Kerusakan Reputasi & Kepercayaan, dan Dampak Sosial & Sistemik. Tren *phishing* kini lebih canggih, tersebar luas, dan menggunakan teknik rekayasa sosial serta AI. Dengan kemampuan AI untuk menyusun konten personalisasi secara otomatis dan realistis, serangan *phishing* kini tidak hanya masif, tetapi juga sangat terarah dan mampu mengelabui pengguna maupun sistem keamanan tradisional. Sebagai bentuk pencegahan terhadap tindak kejahatan *phishing*, dilakukan kegiatan preventif yaitu: dengan melakukan kegiatan pengabdian kepada masyarakat (PkM). Kegiatan PkM ini telah berhasil memberikan penyuluhan dan pendampingan kepada para guru dan siswa SMK N 4 Payakumbuh, dengan materi tentang "Penyuluhan Internet Sehat tentang Bahaya *Phising* dan Dampak Negatifnya bagi Siswa SMK N 4 Payakumbuh". Hasil analisis angket efektivitas kegiatan PkM menunjukkan rata-rata sebesar 82,71%, yang termasuk dalam kategori "baik". Dengan demikian, dapat disimpulkan bahwa pelaksanaan kegiatan PkM dinilai efektif oleh para peserta penyuluhan, dalam hal ini para guru dan beberapa sampel siswa SMK N 4 Payakumbuh.

Kata Kunci : PkM, Penyuluhan Internet Sehat, Bahaya *Phising*, Dampak Negatif *Phising*

Abstract

Phishing is a type of *cybercrime* involving *social engineering* techniques, in which perpetrators impersonate trusted entities such as banks, social media platforms, or government institutions in order to steal sensitive information such as usernames, passwords, credit card details, and other personal data. The impacts of *phishing* attacks are wide-ranging and include: loss of access to personal data and accounts, financial loss, reputational damage and erosion of trust, as well as broader social and systemic consequences. The current trend of *phishing* attacks has evolved to become more sophisticated and widespread, often employing advanced *social engineering* strategies and artificial intelligence (AI). With the ability to automatically generate realistic, personalized content, AI-powered *phishing* campaigns have become not only massive in scale but also highly targeted making it increasingly difficult for users and traditional security systems to detect and counter such threats. As a preventive measure against *phishing* crimes, a community service initiative (PkM-Pengabdian kepada Masyarakat) was conducted. This initiative successfully delivered educational outreach and assistance to teachers and students at SMK N 4 Payakumbuh, with a focus on the topic: "Raising Awareness of Safe Internet Practices and the Dangers of *Phishing* for Vocational High School Students." Based on the analysis of effectiveness surveys distributed after the activity, an average score of 82.71% was achieved, placing the initiative in the "good" category. This suggests that the participants comprising both teachers and a sample of students from SMK N 4 Payakumbuh found the community engagement activity to be effective in increasing awareness and understanding of *phishing* threats.

Keyword : *Community Service Program, Educational Outreach on Safe Internet Practices, Dangers of Phishing, Adverse Effects of Phishing.*

1. PENDAHULUAN

Satu dekade terakhir ini, dunia tengah menghadapi permasalahan serius terkait tindak kejahatan siber, khususnya serangan *phishing* yang semakin kompleks dan masif. *Phishing* adalah metode kejahatan siber (*cybercrime*) berupa *social engineering* di mana pelaku menyamar sebagai entitas terpercaya (bank, media sosial, lembaga pemerintah), untuk mencuri data sensitif seperti *username*, *password*, kartu kredit, dan data pribadi lainnya (Bhavsar et al., 2018). Tindak kejahatan *phishing* menggunakan beberapa tipe meliputi: 1) *Email phishing*, pesan massal yang mengarahkan korban ke situs palsu; 2) *Spear phishing & whaling*: serangan terarah pada individu atau pejabat penting; 3) *Smishing*: *phishing* melalui SMS; 4) *Man-in-the-Middle (MitM)*: intersepsi data meski ada fitur autentikasi dua faktor; dan 5) *Quishing*: *phishing* melalui *QR code* palsu (Putra et al., 2024).

Studi kasus nyata menunjukkan betapa masif dan berkembangnya serangan *phishing*, baik global maupun lokal, diantaranya yaitu 1) Kasus Avalanche (2016) – Skema *Phishing Global*, yang melibatkan 30 negara, termasuk Indonesia. Jaringan siber "Avalanche" memfasilitasi penyebaran *email phishing* dan *malware* (*ransomware*, *trojan*) secara massal. Dampaknya: Lebih dari 500.000 komputer terinfeksi setiap harinya. Sistem digunakan untuk mencuri kredensial dan data perbankan. 2) *Phishing* Tokopedia dan Bukalapak (Indonesia, 2020), dengan modusnya yaitu email dan tautan palsu mengarahkan korban ke halaman login palsu. Dan berdampak pada data akun bocor, penipuan pembelian, dan pencurian identitas. 3) Studi Mahasiswa Universitas di Indonesia (2022), dengan dampak: 28% dari 150 mahasiswa gagal mengenali *email phishing* sehingga memberikan data mereka kepada pihak yang tidak bertanggung jawab.

Studi kasus yang diuraikan dalam paragraf sebelumnya menunjukkan bahwa tindak kejahatan *phishing* dapat menimbulkan berbagai dampak meliputi: 1) Dampak terhadap Data dan Akun Kehilangan akses akun & data pribadi: korban berpotensi kehilangan kontrol atas akun penting email, media sosial, perbankan sehingga data sensitif mudah disalahgunakan (Fadli et al., 2024). 2) Dampak Finansial, Kerugian langsung: korban individu maupun organisasi mengalami kerugian finansial signifikan saat data kartu kredit, rekening, atau kredensial dirampas dan disalahgunakan. 3) Kerusakan Reputasi & Kepercayaan, perusahaan atau individu yang datanya bocor bisa kehilangan reputasi, mengurangi kepercayaan pengguna/klien, serta menurunkan citra institusional. 4) Dampak Sosial & Sistemik, Tingkat kesadaran rendah: Studi mahasiswa menunjukkan 28% responden bisa terkena *phishing* menunjukkan masih banyak yang rentan dan kurang literasi digital (Gumay et al., 2024).

Tren *phishing* kini lebih canggih, tersebar luas, dan menggunakan teknik rekayasa sosial serta AI. *Phishing* berbasis AI kini mampu menghasilkan email dan pesan palsu yang sangat realistis dengan tata bahasa yang tanpa celah, penyusunan struktur yang meyakinkan, dan personalisasi gaya bahasa yang meniru korban secara spesifik. Selain itu, serangan jenis *quishing* melalui kode *QR* juga meningkat, terbukti memiliki tingkat imbas serupa dengan *phishing* tradisional, walaupun cenderung lebih sulit dideteksi oleh sistem proteksi konvensional (Weinz et al., 2025). Lebih lanjut, rekayasa sosial semakin meluas lewat pemanfaatan *deepfake audio* dan video misalnya peniruan suara CEO dalam panggilan video yang berhasil menyulitkan verifikasi identitas dan membuka celah kejahatan finansial hingga jutaan dolar. Dengan kemampuan AI untuk menyusun konten personalisasi secara otomatis dan realistis, serangan *phishing* kini tidak hanya masif, tetapi juga sangat terarah dan mampu mengelabui pengguna maupun sistem keamanan tradisional (Schmitt & Flechais, 2023).

Sebagai bentuk pencegahan terhadap tindak kejahatan *phishing*, dapat dilakukan kegiatan preventif diantaranya yaitu: dengan melakukan kegiatan pengabdian kepada masyarakat (PkM) dalam bentuk penyuluhan tentang pentingnya Internet Sehat tentang Bahaya *Phishing* dan Dampak Negatifnya. Dalam konteks kegiatan PkM ini, kegiatan preventif ditujukan kepada guru dan siswa di SMK Negeri 4

Payakumbuh, dengan mempertimbangkan hasil studi kasus yang menunjukkan bahwa bahkan pada tingkat mahasiswa pun masih terdapat kerentanan terhadap serangan *phishing*, sehingga risiko pada siswa sekolah menengah atas dan jenjang yang lebih rendah diperkirakan lebih tinggi.

2. METODE

Metode Pengabdian

Kegiatan pengabdian kepada masyarakat ini dilaksanakan melalui metode penyuluhan dan pendampingan (Khomarudin, Novita, Aulia, et al., 2023). Dalam pelaksanaannya, digunakan dua pendekatan, yaitu pendekatan klasikal dan pendekatan diskusi. Pendekatan klasikal digunakan dalam sesi penyuluhan untuk memberikan edukasi mengenai pentingnya Internet Sehat tentang Bahaya *Phising* dan Dampak Negatifnya. Sementara itu, pendekatan individual diterapkan dalam sesi pendampingan, yang bertujuan untuk melakukan diskusi dalam kelompok kecil serta menggali informasi atau masalah atau kasus dari para peserta kegiatan, yakni para Guru dan siswa SMK N 4 Payakumbuh (Asnawi et al., 2021).

Tahapan Pengabdian

Tahapan kegiatan PkM mulai dari awal sampai dengan akhir, dideskripsikan melalui gambar berikut:



Gambar 1. Tahapan Pelaksanaan Kegiatan PkM

Gambar 1 menggambarkan beberapa langkah yang dilakukan dalam kegiatan Pengabdian kepada Masyarakat (PkM) (Khomarudin, Novita, & Aulia, 2023), yang terdiri dari: **1). Tahap Persiapan.** Pada tahap awal pelaksanaan kegiatan PkM ini dilakukan berbagai persiapan penting, seperti pemilihan lokasi dan kelompok sasaran untuk kegiatan penyuluhan, penyiapan peralatan dan bahan yang dibutuhkan, pengajuan izin pemakaian ruangan pelatihan, pengurusan surat tugas dari institusi penyelenggara PkM, serta penyusunan materi penyuluhan selama kegiatan berlangsung.

2). Tahap Pelaksanaan kegiatan, pada tahap ini terdapat tiga sesi utama, yaitu: (1) Penyampaian materi dalam bentuk presentasi atau penyuluhan, dan (2) Sesi pendampingan serta diskusi dalam kelompok kecil yang terdiri dari para peserta PkM, yaitu guru dan siswa SMK N 4 Payakumbuh. Kegiatan ini bertujuan untuk menggali informasi, mengidentifikasi permasalahan, serta merumuskan solusi atas permasalahan yang ditemukan. (3) Sesi pengisian kuisioner yang menggunakan media *Google Form* dengan tautan tertentu (Ifroh & Permana, 2021).

3). Tahap Evaluasi Pelaksanaan Kegiatan, Proses evaluasi dilakukan untuk memperoleh umpan balik atas kegiatan PkM yang telah dilaksanakan. Informasi ini penting untuk menilai sejauh mana efektivitas kegiatan tersebut. Selain itu, evaluasi ini juga bertujuan untuk menghimpun masukan serta saran sebagai bahan perbaikan dan penyempurnaan program PkM pada pelaksanaan berikutnya (Gusteti et al., 2022).

Sasaran dan Tujuan kegiatan Pengabdian

Sasaran dari kegiatan Pengabdian kepada Masyarakat (PkM) ini adalah pelaksanaan penyuluhan yang ditujukan kepada para guru dan siswa SMK N 4 Payakumbuh. Tujuan dari kegiatan ini antara lain: 1). Meningkatkan pemahaman para guru tentang pentingnya peran mereka dalam membimbing serta melindungi generasi muda dari bahaya phising dan dampak negatifnya; 2). Menumbuhkan kesadaran di kalangan siswa SMK N 4 Payakumbuh mengenai risiko dan bahaya yang dapat ditimbulkan oleh tindak kejahatan phising; 3). Melakukan pendampingan kepada guru dan siswa dalam menggali berbagai informasi serta potensi persoalan yang dihadapi, sekaligus mencari solusi bersama guna mengatasi tindak kejahatan *phising*.

3. HASIL DAN PEMBAHASAN**Hasil Pelaksanaan PkM**

Kegiatan Pengabdian kepada Masyarakat (PkM) yang berbentuk penyuluhan dengan tema “Penyuluhan Internet Sehat tentang Bahaya Phising dan Dampak Negatifnya bagi Siswa SMK N 4 Payakumbuh” diselenggarakan melalui tiga tahapan, yaitu: tahap perencanaan atau persiapan, tahap pelaksanaan, dan tahap evaluasi kegiatan.

1). **Tahap Persiapan**, Tahapan ini diawali dengan menyiapkan seluruh kebutuhan yang diperlukan untuk pelaksanaan kegiatan PkM. Persiapan tersebut meliputi penetapan lokasi dan sasaran penyuluhan, melakukan survei lapangan serta pengajuan izin kepada pihak terkait di lokasi yang dituju, pengurusan surat tugas dari institusi pelaksana, serta penyediaan perlengkapan dan media yang akan digunakan dalam penyuluhan, seperti laptop, proyektor, perangkat pengeras suara, dan konsumsi bagi peserta saat kegiatan berlangsung. Selain itu, dalam tahap ini juga disusun materi penyuluhan yang akan menjadi topik utama selama pelaksanaan kegiatan. Tim pelaksana PkM melakukan diskusi bersama untuk menyusun materi tentang bahaya tindak kejahatan *phising* dan dampak negatifnya bagi siswa SMK.

2). **Tahap Pelaksanaan Kegiatan PkM**, Tahapan pelaksanaan kegiatan PkM terdiri dari tiga bagian utama, yaitu: (a) Penyampaian materi melalui sesi penyuluhan bertema “Penyuluhan Internet Sehat tentang Bahaya Phising dan Dampak Negatifnya bagi Siswa SMK N 4 Payakumbuh” yang disampaikan oleh para mahasiswa program studi D4-Teknologi Rekayasa Komputer, Politeknik Pertanian Negeri Payakumbuh; (b) Sesi pendampingan serta diskusi kelompok kecil yang melibatkan para guru dan siswa SMK N 4 Payakumbuh sebagai peserta, dengan tujuan untuk menggali informasi, mengidentifikasi potensi permasalahan, serta merumuskan solusi bersama guna mengatasi tindak kejahatan *phising*; (c) Sesi selanjutnya yaitu pengisian kuisioner yang menggunakan media *Google Form* dengan tautan tertentu. Dokumentasi kegiatan PkM ini dapat ditampilkan pada gambar 2 berikut:



Gambar 2. Dokumentasi proses pemaparan materi dan diskusi atau review materi

3). **Tahap Evaluasi Kegiatan PkM**, Kegiatan evaluasi dilakukan untuk mendapatkan *feedback* dari pelaksanaan PkM ini yang berguna dalam analisis terkait keefektifan kegiatan PkM yang telah dilakukan. Pada tahap evaluasi kegiatan PkM dilakukan dengan cara menyebarkan angket efektifitas

pelaksanaan kegiatan PkM, dalam konteks ini yaitu kepada para guru dan beberapa sampel siswa SMK N 4 Payakumbuh. Angket efektifitas pelaksanaan kegiatan PkM berisi 10 aspek penilaian yang terkait dengan pelaksanaan kegiatan PkM. Angket efektifitas pelaksanaan kegiatan PkM yang telah diisi oleh para guru dan beberapa sampel siswa SMK N 4 Payakumbuh, selanjutnya dilakukan pengolahan menggunakan alat bantu atau aplikasi pengolah angka dengan hasil seperti pada tabel 1 berikut:

Tabel 1. Rekapitulasi Hasil Angket Efektivitas Kegiatan PkM

No	Indikator	Hasil (%)
1	Kegiatan PkM yang dilaksanakan dinilai telah sesuai dengan harapan para peserta	83,33%
2	Penyampaian materi oleh narasumber dianggap menarik oleh peserta	85,42%
3	Isi materi penyuluhan PkM dipahami dengan mudah dan disampaikan secara jelas	81,25%
4	Alokasi waktu yang diberikan dinilai cukup untuk penyampaian materi	77,08%
5	Mitra menunjukkan minat untuk terlibat dalam kegiatan PkM selama kegiatan tersebut sesuai dengan kebutuhan mereka	87,50%
6	Seluruh anggota tim PkM aktif berpartisipasi dan memberikan pelayanan sesuai dengan kebutuhan mitra	83,33%
7	Kegiatan PkM dinilai memiliki kesinambungan dan dilakukan secara berkelanjutan	81,25%
8	Setiap pertanyaan, keluhan, atau masalah yang disampaikan oleh peserta ditanggapi dengan baik oleh tim PkM	85,42%
9	Mitra merasakan manfaat secara langsung dari pelaksanaan kegiatan PkM	81,25%
10	Secara keseluruhan, mitra merasa puas terhadap kegiatan PkM yang telah dilaksanakan	81,25%
Rata-rata Skor		82,71%
Kategori Penilaian		Baik

Merujuk pada Tabel 1, hasil analisis angket efektivitas kegiatan PkM menunjukkan rata-rata sebesar 82,71%, yang termasuk dalam kategori "baik". Dengan demikian, dapat disimpulkan bahwa pelaksanaan kegiatan PkM dinilai efektif oleh para peserta penyuluhan, dalam hal ini para guru dan beberapa sampel siswa SMK N 4 Payakumbuh.

Pembahasan

Kegiatan PkM ini telah berhasil memberikan penyuluhan dan pendampingan kepada para guru dan siswa SMK N 4 Payakumbuh, dengan materi tentang "Penyuluhan Internet Sehat tentang Bahaya *Phising* dan Dampak Negatifnya bagi Siswa SMK N 4 Payakumbuh". *Phishing* merupakan bentuk kejahatan siber yang melibatkan upaya penipuan untuk memperoleh informasi sensitif seperti nama pengguna, kata sandi, dan data kartu kredit dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik. Serangan ini sering dilakukan melalui email, pesan instan, atau situs *web* palsu yang dirancang menyerupai situs resmi.

Tindak kejahatan *phising* dapat menimbulkan berbagai dampak meliputi: 1) Dampak terhadap Data dan Akun Kehilangan akses akun & data pribadi: korban berpotensi kehilangan kontrol atas akun penting email, media sosial, perbankan sehingga data sensitif mudah disalahgunakan. 2) Dampak Finansial, Kerugian langsung: korban individu maupun organisasi mengalami kerugian finansial

signifikan saat data kartu kredit, rekening, atau kredensial dirampas dan disalahgunakan. 3) Kerusakan Reputasi & Kepercayaan, perusahaan atau individu yang datanya bocor bisa kehilangan reputasi, mengurangi kepercayaan pengguna/klien, serta menurunkan citra institusional. 4) Dampak Sosial & Sistemik, Tingkat kesadaran rendah: Studi mahasiswa menunjukkan 28% responden bisa terkena phishing menunjukkan masih banyak yang rentan dan kurang literasi digital.

Tren *phishing* kini lebih canggih, tersebar luas, dan menggunakan teknik rekayasa sosial serta AI. *Phishing* berbasis AI kini mampu menghasilkan email dan pesan palsu yang sangat realistis dengan tata bahasa yang tanpa celah, penyusunan struktur yang meyakinkan, dan personalisasi gaya bahasa yang meniru korban secara spesifik. Selain itu, serangan jenis *quishing* melalui kode *QR* juga meningkat, terbukti memiliki tingkat imbas serupa dengan *phishing* tradisional, walaupun cenderung lebih sulit dideteksi oleh sistem proteksi konvensional (Weinz et al., 2025). Lebih lanjut, rekayasa sosial semakin meluas lewat pemanfaatan *deepfake audio* dan video misalnya peniruan suara CEO dalam panggilan video yang berhasil menyulitkan verifikasi identitas dan membuka celah kejahatan finansial hingga jutaan dolar. Dengan kemampuan AI untuk menyusun konten personalisasi secara otomatis dan realistis, serangan phishing kini tidak hanya masif, tetapi juga sangat terarah dan mampu mengelabui pengguna maupun sistem keamanan tradisional (Schmitt & Flechais, 2023).

Kegiatan pengabdian kepada masyarakat (PkM) dalam bentuk penyuluhan tentang pentingnya Internet Sehat tentang Bahaya *Phising* dan Dampak Negatifnya ini merupakan bentuk pencegahan atau tindakan preventif terhadap tindak kejahatan *phising* bagi kalangan remaja. Dalam konteks kegiatan PkM ini, kegiatan preventif ditujukan kepada guru dan siswa di SMK Negeri 4 Payakumbuh, dengan mempertimbangkan hasil studi kasus yang menunjukkan bahwa bahkan pada tingkat mahasiswa pun masih terdapat kerentanan terhadap serangan *phishing*, sehingga risiko pada siswa sekolah menengah atas dan jenjang yang lebih rendah diperkirakan lebih tinggi.

4. KESIMPULAN

Satu dekade terakhir ini, dunia tengah menghadapi permasalahan serius terkait tindak kejahatan siber, khususnya serangan *phishing* yang semakin kompleks dan masif. *Phishing* adalah metode kejahatan siber (*cybercrime*) berupa *social engineering* di mana pelaku menyamar sebagai entitas terpercaya (bank, media sosial, lembaga pemerintah), untuk mencuri data sensitif seperti *username*, *password*, kartu kredit, dan data pribadi lainnya.

Kegiatan pengabdian kepada masyarakat (PkM) dalam bentuk penyuluhan ini merupakan bentuk pencegahan atau tindakan preventif terhadap tindak kejahatan *phising* bagi kalangan remaja, terkhusus ditujukan kepada para siswa di SMK Negeri 4 Payakumbuh agar terhindar dari tindak kejahatan atau serangan *phishing*. Hasil analisis angket efektivitas kegiatan PkM menunjukkan rata-rata sebesar 82,71%, yang termasuk dalam kategori "baik". Dengan demikian, dapat disimpulkan bahwa pelaksanaan kegiatan PkM dinilai efektif oleh para peserta penyuluhan, dalam hal ini para guru dan beberapa sampel siswa SMK N 4 Payakumbuh.

5. UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya kegiatan PkM ini, meliputi: Mahasiswa Prodi D4-Teknologi Rekayasa Komputer, Politeknik Pertanian Negeri Payakumbuh. Selanjutnya ucapan terimakasih kepada tim Dosen Pendamping dan tentunya tidak lupa kami berterima kasih kepada Pihak SMK N 4 Payakumbuh yang telah berkenan meluangkan waktu dan menyediakan tempat lokasi untuk kegiatan PkM ini.

6. DAFTAR PUSTAKA

- Asnawi, A., Wahyuni, S., Alber, A., & Etfita, F. (2021). Pelatihan Manajemen Referensi Menggunakan Mendeley Untuk Menulis Artikel Ilmiah Bagi Guru-Guru Mgmmp Smp Negeri Di Pekanbaru. *Jurnal Dedikasia : Jurnal Pengabdian Masyarakat*, 1(2), 148. <https://doi.org/10.30983/Dedikasia.V1i2.5148>
- Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study On Phishing Attacks. *International Journal Of Computer Applications*, 182(33), 27–29. <https://doi.org/10.5120/Ijca2018918286>
- Fadli, M., Widiyowati, D., & Andayani, D. (2024). Pencurian Data Pribadi Di Dunia Maya (Phising Cybercrime) Yang Ditinjau Dalam Perspektif Kriminologi. *Co-Value: Jurnal Ekonomi, Koperasi Dan Kewirausahaan*, 14(12). <https://doi.org/10.59188/Covalue.V14i1.4335>
- Gumay, B., Hendrawan, A. H., Satrya, F., Kusumah, F., Informatika, T., & Khaldun, U. I. (2024). Analisis Dampak Ancaman Cybercrime Terhadap Data Mahasiswa Pada Serangan Web Phising Siak Uika. *Infotech Journal*, 10(2), 297–305.
- Gusteti, M. U., Handayani, D. F., Mutiara, N., Delvia, R., & Putri, M. (2022). Pelatihan Membuat Video Pembelajaran Dengan Smartphone Untuk Meningkatkan Kompetensi Guru-Guru Sd Di Pesisir Selatan. *Jurnal Dedikasia : Jurnal Pengabdian Masyarakat*, 2(1), 41. <https://doi.org/10.30983/Dedikasia.V2i1.5508>
- Ifroh, R. H., & Permana, L. (2021). Pelatihan Pembuatan Media Audiovisual Dalam Meningkatkan Kemampuan Kreatif Digital Remaja. *Jurnal Pengabdian Pada Masyarakat*, 6(4), 1158–1165. <https://doi.org/10.30653/002.202164.867>
- Khomarudin, A. N., Novita, R., & Aulia, R. (2023). *Penyuluhan Dan Pendampingan Kepada Guru Dan Siswa MdtA Tentang Arif Dan Bijak Dalam Penggunaan Smartphone*. 1, 46–56.
- Khomarudin, A. N., Novita, R., Aulia, R., & Putri, E. E. (2023). Workshop E-Learning Kepada Guru Tk Dan Sd Excellent Bukittinggi Sebagai Upaya Peningkatan Kemampuan Profesional Dan Digital. *Journal Of Indonesian Social Society (Jiss)*, 1(2), 54–59. <https://doi.org/10.59435/Jiss.V1i2.81>
- Putra, F. P. E., Ubaidi, U., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis Of Phishing Attack Trends, Impacts And Prevention Methods: Literature Study. *Brilliance: Research Of Artificial Intelligence*, 4(1), 413–421. <https://doi.org/10.47709/Brilliance.V4i1.4357>
- Schmitt, M., & Flechais, I. (2023). Digital Deception: Generative Artificial Intelligence In Social Engineering And Phishing. *Ssm Electronic Journal*. <https://doi.org/10.2139/Ssm.4602790>
- Weinz, M., Zannone, N., Allodi, L., & Apruzzese, G. (2025). The Impact Of Emerging Phishing Threats: Assessing Quishing And Llm-Generated Phishing Emails Against Organizations. In *Acm Asia Conference On Computer And Communications Security (Asia Ccs '25)*, August 25â •fi29, 2025, Hanoi, Vietnam (Vol. 1, Issue 1). Arxiv. <https://doi.org/10.1145/3708821.3736195>