At-Ta'lim: Journal of Community Service
E-ISSN 3110-5785
Vol 2, No. 1, 2026, pp. 7-15

PELATIHAN KEAMANAN DATA UNTUK MENINGKATKAN KEWASPADAAN TERHADAP SERANGAN SIBER DAN PENIPUAN DI PKBM KAMPOENG ILMU CENTER

Dyah Ayu Nurmumpuni[1*], Hananing Sumaningdiah Larasati[2], Rizky Fauzi[3]
[1, 2, 3] Program Studi Sistem Informasi, Universitas Pamulang, Tangerang Selatan, Indonesia
dosen03310@unpam.ac.id, Dosen02819@unpam.ac.id, dosen02810@unpam.ac.id

Abstract

This community service activity (PKM) aims to enhance data security awareness and digital literacy among suburban learners. Objectives: To evaluate and improve cybersecurity awareness and data protection skills among students in a non-formal education setting. Methods: A structured, interactive workshop approach was implemented, including situational analysis, pre-test evaluation, practical simulations of password strengthening and two-factor authentication (2FA) setup, post-test assessment, and monitoring. Results: The intervention significantly improved participant understanding, as reflected in the average score increase from 45% (pre-test) to 88% (post-test), alongside high practical compliance in securing personal devices. Conclusion: Integrating hands-on technical guidance with digital ethical awareness is a highly effective model to reduce cyber vulnerability in non-formal education communities. Contribution: This research establishes a practical community-based framework for cyber safety education that incorporates technological hygiene with digital responsibility.
Keyword: cybersecurity, digital literacy, non-formal education, two-factor authentication, phishing.

Abstract

Kegiatan pengabdian kepada masyarakat (PKM) ini bertujuan untuk meningkatkan kewaspadaan keamanan data dan literasi digital di kalangan peserta didik pendidikan nonformal. Tujuan: Untuk menganalisis dan meningkatkan kesadaran siber serta keterampilan perlindungan data warga belajar Paket C di PKBM Kampoeng Ilmu Center. Metode: Pelatihan interaktif terstruktur yang meliputi analisis situasi, evaluasi awal (pre-test), simulasi praktik penguatan kata sandi dan verifikasi dua langkah (2FA), serta evaluasi akhir (post-test). Hasil: Pelaksanaan program ini menunjukkan peningkatan pemahaman siber peserta secara signifikan, di mana nilai rata-rata meningkat dari 45% (pre-test) menjadi 88% (post-test) serta terwujudnya kemandirian dalam mengamankan perangkat komunikasi pribadi. Kesimpulan: Penyediaan bimbingan teknis langsung yang dipadukan dengan penguatan kesadaran etika digital merupakan pendekatan yang sangat efektif dalam menekan kerentanan siber. Kontribusi: Menyajikan kerangka kerja pelatihan keamanan data berbasis komunitas yang mensinergikan aspek teknis dengan nilai tanggung jawab etika digital.
Kata Kunci: *keamanan siber, literasi digital, pendidikan nonformal, verifikasi dua langkah, phishing.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era globalisasi saat ini telah membawa perubahan paradigma yang sangat fundamental dalam seluruh aspek kehidupan manusia. Berbagai kemudahan akses yang ditawarkan oleh internet telah mentransformasikan cara masyarakat berkomunikasi, belajar, bekerja, hingga melakukan transaksi keuangan. Namun, di balik efisiensi dan kenyamanan tersebut, terdapat tantangan keamanan informasi yang sangat kompleks dan berpotensi membahayakan data pribadi pengguna. Ketergantungan masyarakat terhadap teknologi digital yang semakin tinggi sering kali tidak diimbangi dengan tingkat pemahaman dan kesadaran mengenai pentingnya perlindungan data, khususnya di kalangan peserta didik nonformal di wilayah suburban (Ahmadi & Hermawan, 2021). Banyak pengguna internet yang belum memprioritaskan langkah-langkah keamanan dasar seperti penggunaan kata sandi yang kuat dan unik, sehingga rentan menjadi korban kejahatan siber.

Dalam lingkup akademis dan praktis sistem informasi, kerangka kerja keamanan informasi bersandar pada tiga pilar utama yang dikenal sebagai Triad CIA: kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Kerahasiaan memastikan data sensitif hanya diakses oleh pihak berwenang, integritas menjamin keakuratan informasi dari manipulasi pihak luar, dan ketersediaan menjamin akses data yang sah dapat diperoleh saat dibutuhkan (Pratama, 2021). Kendati infrastruktur keamanan siber dikembangkan dengan teknologi enkripsi tercanggih, faktor manusia tetap diakui sebagai mata rantai terlemah (the weakest link) dalam sistem pertahanan tersebut. Serangan siber modern, terutama phishing dan rekayasa sosial (social engineering), sengaja memanfaatkan kelemahan psikologis dan kelengahan pengguna untuk mencuri data pribadi seperti kredensial akun, kode OTP, dan nomor identifikasi penting (Novitasari, 2025).

Di Indonesia, tingkat kesadaran keamanan siber masyarakat marginal dan peserta didik di lembaga nonformal seperti Pusat Kegiatan Belajar Masyarakat (PKBM) masih berada pada kategori yang sangat minim. PKBM Kampoeng Ilmu Center yang berlokasi di Kecamatan Setu, Kota Tangerang Selatan, Banten, merupakan salah satu wadah pendidikan nonformal Paket A, B, dan C yang berfokus pada pemberdayaan warga belajar yang putus sekolah atau memiliki keterbatasan ekonomi. Meskipun warga belajar aktif menggunakan smartphone dalam kegiatan sehari-hari untuk hiburan dan komunikasi sosial, tingkat literasi digital mereka masih sebatas pada penggunaan aplikasi umum tanpa memahami risiko keamanan informasi yang mengintai mereka (Hidayat, 2022). Hasil survei awal di PKBM Kampoeng Ilmu Center menunjukkan bahwa sebagian besar peserta didik menggunakan satu kata sandi yang sama dan mudah ditebak untuk berbagai platform, tidak mengaktifkan fitur verifikasi dua langkah (2FA), serta belum mampu mendeteksi indikasi penipuan daring berbasis link phishing.

Bila ditinjau dari perspektif etika digital dan nilai-nilai moral kemasyarakatan, perlindungan data pribadi dan kewaspadaan siber erat kaitannya dengan nilai

tanggung jawab pribadi (amanah) dan proses konfirmasi berita (tabayyun). Dalam menghadapi era disrupsi informasi serta maraknya kejahatan rekayasa sosial, penerapan konsep tabayyun—yaitu memverifikasi kebenaran dan keabsahan informasi sebelum bertindak atau menyebarkannya—merupakan pertahanan kognitif utama untuk menangkal taktik manipulasi psikologis penipu siber (Hafidh, 2020). Demikian pula dengan menjaga kerahasiaan kata sandi dan kredensial akun yang merupakan amanah pribadi untuk mencegah timbulnya kerugian bagi diri sendiri maupun orang lain (Wardhana, 2023). Oleh karena itu, edukasi keamanan data berbasis komunitas di PKBM tidak hanya penting dari sisi penguasaan aspek teknologi teknis, melainkan juga dari penguatan etika moral dan perilaku bijak dalam beraktivitas di ruang digital.

Berdasarkan analisis situasi tersebut, tim Pengabdian kepada Masyarakat (PKM) dari Program Studi Sistem Informasi Universitas Pamulang merancang program intervensi berupa pelatihan terstruktur dengan judul "Pelatihan Keamanan Data untuk Meningkatkan Kewaspadaan terhadap Serangan Cyber dan Penipuan di PKBM Kampoeng Ilmu Center". Program ini bertujuan untuk memberikan landasan pengetahuan siber yang kokoh, membekali keterampilan praktis dalam mengamankan perangkat pribadi, dan membangun budaya digital yang sehat berlandaskan etika siber. Melalui kegiatan ini, diharapkan warga belajar Paket C di PKBM tersebut mampu bertransformasi menjadi agen edukasi literasi digital di lingkungan keluarga dan masyarakat sekitarnya.

METODE

Kegiatan pengabdian masyarakat ini menggunakan pendekatan intervensi edukatif berbasis tindakan partisipatif (participatory action research) untuk memastikan transfer pengetahuan dan keterampilan berlangsung secara efektif (Wijaya & Kusuma, 2024). Metode pelaksanaan dirancang melalui empat tahapan utama yang sistematis: (1) Persiapan dan koordinasi wilayah mitra; (2) Asesmen awal melalui instrumen pre-test; (3) Pelaksanaan pelatihan interaktif yang mengkombinasikan penyampaian teori dan simulasi praktik langsung; serta (4) Evaluasi akhir melalui instrumen post-test dan monitoring kepatuhan pasca-kegiatan.

Pelatihan dilaksanakan pada hari Minggu, 26 Oktober 2025, bertempat di Ruang Kelas PKBM Kampoeng Ilmu Center, yang berlokasi di perumahan Citra Prima Serpong, RT.02/RW.04, Kelurahan Kademangan, Kecamatan Setu, Kota Tangerang Selatan, Provinsi Banten. Khalayak sasaran atau subjek kegiatan ini adalah warga belajar Program Kesetaraan Paket C yang berjumlah 20 orang. Pemilihan hari Minggu didasarkan pada kesepakatan bersama mitra karena sebagian besar warga belajar merupakan pekerja usia produktif yang hanya memiliki waktu luang di akhir pekan.

Pengumpulan data dilakukan dengan menyebarkan kuesioner pre-test sebelum penyampaian materi guna mengukur pemahaman awal peserta terhadap konsep dasar siber. Kuesioner terdiri dari 10 butir pertanyaan pilihan ganda yang mencakup aspek kerahasiaan kata sandi, deteksi tautan phishing, bahaya malware, pentingnya 2FA, dan bahaya rekayasa sosial (Setyawan & Wibowo, 2023). Setelah sesi pelatihan selesai, instrumen post-test dengan bobot dan jenis soal yang setara dibagikan kembali kepada

peserta untuk menganalisis efektivitas pelatihan. Selain itu, lembar observasi digunakan untuk mencatat keberhasilan teknis peserta saat mempraktikkan pembuatan kata sandi kuat menggunakan metode mnemonik dan langkah mengaktifkan 2FA pada akun media sosial atau email pribadi mereka secara langsung.

Analisis data hasil kegiatan menggunakan statistik deskriptif komparatif dengan membandingkan persentase perolehan nilai rata-rata pre-test dan post-test untuk mengetahui tingkat peningkatan pemahaman (gain score) warga belajar. Data kualitatif yang diperoleh dari pengamatan aktivitas diskusi serta simulasi praktik disintesiskan secara naratif untuk memberikan gambaran komprehensif mengenai tingkat antusiasme, hambatan teknis yang dihadapi, serta perubahan perilaku digital warga belajar setelah mengikuti rangkaian pelatihan keamanan informasi (UNESCO, 2020).

HASIL KEGIATAN

Pelaksanaan kegiatan PKM ini terbagi ke dalam tiga fase utama yang berjalan dengan lancar. Pertama, fase persiapan dimulai dengan melakukan survei awal dan koordinasi bersama Bapak Fiqhi Farabi selaku Kepala Sekolah PKBM Kampoeng Ilmu Center. Pada tahap ini, tim dosen dan mahasiswa menyusun modul pelatihan bertajuk "Panduan Higiene Digital dan Proteksi Akun Mandiri" serta merancang instrumen evaluasi. Selanjutnya, briefing internal panitia dilakukan untuk memastikan pembagian tugas asistensi personal selama simulasi praktik berjalan optimal.

Kedua, fase pelaksanaan diawali dengan pembagian lembar pre-test. Setelah itu, penyampaian materi edukatif dilakukan secara bertahap dalam tiga sesi utama: Sesi 1 mengenalkan dasar keamanan informasi dan jenis ancaman digital; Sesi 2 mengupas "senjata" rekayasa sosial seperti link phishing dan manipulasi OTP; dan Sesi 3 memfokuskan pada langkah-langkah praktis pencegahan mandiri. Sesi 3 melibatkan demonstrasi interaktif pembuatan kata sandi yang kuat dan simulasi pengaktifan fitur 2FA pada akun email dan WhatsApp masing-masing peserta secara langsung dengan bimbingan intensif dari tim pengabdi.

Ketiga, fase evaluasi diakhiri dengan pengerjaan post-test oleh seluruh peserta yang hadir (20 orang). Hasil dari pengumpulan kuesioner pre-test dan post-test dianalisis dan dikelompokkan berdasarkan kategori evaluasi keamanan informasi. Data perbandingan persentase pemahaman rata-rata peserta sebelum dan sesudah pelatihan dapat dilihat secara detail pada Tabel 1 di bawah ini.

Tabel 1. Skor Kemampuan Siswa Sebelum dan Sesudah Pelatihan Keamanan Data

No.	Kategori Evaluasi	Pre-test (%)	Post-test (%)	Peningkatan (%)
1	Kerahasiaan Kata Sandi (Password)	50	90	40
2	Deteksi Phishing &	35	85	50

	Tautan Palsu			
3	Pemahaman Malware & Aplikasi Berbahaya	40	85	45
4	Aktivasi Verifikasi Dua Langkah (2FA)	20	80	60
5	Bahaya Rekayasa Sosial & Proteksi OTP	45	90	45
6	Higiene Perangkat Digital (Device Hygiene)	55	95	40

Berdasarkan Tabel 1, terlihat adanya peningkatan pemahaman yang sangat signifikan pada seluruh aspek evaluasi keamanan digital. Peningkatan tertinggi tercatat pada kategori Aktivasi Verifikasi Dua Langkah (2FA) sebesar 60%, di mana persentase kemampuan awal peserta hanya 20% karena sebagian besar belum pernah mendengar istilah 2FA atau mengetahui fungsinya. Kategori Deteksi Phishing dan Tautan Palsu juga menunjukkan kenaikan yang memuaskan sebesar 50%, membuktikan bahwa pelatihan simulasi pengenalan domain url palsu memberikan pemahaman konkret bagi warga belajar dalam menyaring informasi yang mencurigakan.

PEMBAHASAN

Keberhasilan program pelatihan ini didukung oleh metode pembelajaran interaktif yang tidak hanya berfokus pada teori satu arah, melainkan pada praktik terbimbing (hands-on) secara personal. Edukasi keamanan siber bagi warga belajar Paket C memiliki tantangan tersendiri karena perbedaan latar belakang usia dan tingkat penguasaan teknologi dasar. Oleh karena itu, pendekatan diskusi kasus nyata (seperti pembajakan akun WhatsApp tokoh terkenal atau penipuan berkedok kurir paket online) terbukti lebih mudah dicerna oleh peserta dibandingkan penjelasan definisi teknis yang abstrak (Kurniawan & Saputra, 2022). Hal ini sejalan dengan temuan Hartanto et al. (2024) yang menyatakan bahwa edukasi berbasis studi kasus nyata dapat merangsang ketertarikan peserta didik untuk segera mengamankan akun pribadi mereka.

Pilar Triad CIA dalam penelitian ini dioperasionalkan melalui langkah pencegahan mandiri yang diajarkan pada Sesi 3. Warga belajar diajarkan cara membuat kata sandi yang memenuhi standar kerahasiaan (confidentiality) menggunakan kombinasi huruf besar, kecil, angka, dan simbol unik. Melalui metode mnemonik yang sederhana, peserta dapat membuat kata sandi yang mudah diingat oleh diri sendiri tetapi sangat sulit ditebak oleh serangan brute force (Setyawan & Wibowo, 2023). Selain itu, untuk menjaga aspek integritas (integrity) akun dari pembajakan, aktivasi verifikasi dua langkah (2FA) dipraktikkan langsung. Dengan 2FA aktif, meskipun peretas berhasil menebak kata sandi, mereka tetap tidak dapat mengakses akun tanpa kode verifikasi tambahan yang dikirimkan ke perangkat fisik pemilik sah (Azkiya et al., 2024).

Menariknya, integrasi nilai-nilai moral keagamaan berupa konsep tabayyun dan amanah terbukti mampu memperkuat pemahaman etis warga belajar dalam berperilaku di dunia maya. Konsep tabayyun (QS. Al-Hujurat: 6) yang bermakna proses penelitian, verifikasi, dan konfirmasi informasi diaplikasikan sebagai benteng pertahanan psikologis utama dalam mendeteksi upaya phishing dan rekayasa sosial (social engineering). Dalam konteks keamanan digital, tabayyun mewajibkan pengguna untuk bersikap kritis terhadap pesan tidak dikenal yang meminta data sensitif atau tautan yang memanipulasi emosi korban (seperti ketakutan akun akan diblokir atau iming-iming hadiah) (Hafidh, 2020). Dengan melatih kebiasaan tabayyun digital, peserta belajar menyaring informasi secara mandiri sebelum memberikan data pribadi mereka (Yasir & Anwar, 2023). Sementara itu, menjaga kredensial login akun diposisikan sebagai pemenuhan kewajiban amanah (QS. Al-Anfal: 27) untuk melindungi privasi diri serta menghindari penyalahgunaan akun oleh peretas untuk menipu orang lain (Wardhana, 2023).

Bila dibandingkan dengan penelitian terdahulu, studi Yudistira et al. (2025) dan Farahanita et al. (2022) lebih banyak menitikberatkan pada aspek sosialisasi teoritis tanpa adanya pendampingan teknis secara privat. Kelemahan pendekatan tersebut adalah peserta cenderung lupa dan tidak menindaklanjuti rekomendasi keamanan pasca-pelatihan. Sebaliknya, pelatihan yang kami lakukan di PKBM Kampoeng Ilmu Center menjamin bahwa 100% peserta pulang dengan kondisi akun WhatsApp dan email mereka telah terproteksi oleh verifikasi dua langkah. Hal ini menegaskan bahwa edukasi keamanan siber bagi kelompok masyarakat marginal harus menyentuh aspek pendampingan teknis langsung untuk memicu perubahan perilaku digital yang instan dan permanen (Ramadhan & Fitriani, 2024).

Meskipun hasil yang diperoleh sangat positif, beberapa warga belajar yang berusia lebih tua awalnya mengalami kendala teknis dalam memahami menu pengaturan keamanan di smartphone mereka karena perbedaan antarmuka sistem operasi (Android vs iOS). Peran asistensi mahasiswa pengabdi sangat krusial dalam mengatasi hambatan ini dengan memberikan panduan langkah-demi-langkah secara personal. Secara keseluruhan, integrasi aspek pemahaman teoretis keamanan siber, simulasi teknis praktis, dan internalisasi etika moral digital terbukti berhasil membangun

kesadaran siber yang komprehensif bagi warga belajar Paket C PKBM Kampoeng Ilmu Center (Sari & Utami, 2021).

Penelitian pengabdian ini memiliki beberapa implikasi penting. Pertama, implikasi praktis berupa terbentuknya kemampuan mandiri pada warga belajar dalam memitigasi risiko kejahatan siber, sehingga menurunkan potensi kerugian material maupun moral akibat pembajakan akun dan penipuan daring. Kedua, implikasi teoritis yang menyajikan model integrasi antara literasi keamanan informasi (Triad CIA) dengan etika moral keagamaan (tabayyun dan amanah) sebagai landasan teoretis baru dalam merancang program edukasi teknologi bagi masyarakat. Ketiga, implikasi metodologis yang membuktikan efektivitas evaluasi pre-test dan post-test yang dikombinasikan dengan pendampingan langsung (hands-on) dalam meningkatkan retensi pemahaman siber peserta pelatihan (Wijaya & Kusuma, 2024).

Penelitian ini memberikan kontribusi nyata terhadap pengembangan ilmu pengetahuan di bidang sistem informasi, khususnya terkait studi perilaku keamanan informasi (information security behavior) pada kelompok masyarakat suburban dan marginal. Secara khusus, kontribusi terbesar program ini adalah bagi dunia pendidikan nonformal (pendidikan kesetaraan Paket C) dengan menyediakan modul higiene digital terstandar yang mudah diadaptasi dan diintegrasikan ke dalam kurikulum pembelajaran PKBM. Hal ini mendukung upaya pemerataan literasi digital yang dicanangkan pemerintah untuk mempersiapkan seluruh lapisan masyarakat menghadapi era Revolusi Industri 5.0 dan Society 5.0 tanpa menyisakan kesenjangan kemampuan perlindungan data pribadi (Ahmadi & Hermawan, 2021).

REKOMENDASI

Meskipun program pelatihan ini terbukti berhasil meningkatkan kesadaran siber warga belajar secara instan, penelitian selanjutnya disarankan untuk melakukan evaluasi jangka panjang (longitudinal study) guna menguji retensi pemahaman dan konsistensi perilaku keamanan informasi peserta setelah periode 3 hingga 6 bulan pasca-pelatihan. Selain itu, materi edukasi di masa depan perlu diperluas dengan mencakup topik keamanan transaksi keuangan digital (financial technology/fintech awareness), mengingat semakin maraknya kasus pinjaman online ilegal dan judi online yang menargetkan masyarakat kelas menengah ke bawah. Terakhir, replikasi program pelatihan disarankan untuk diperluas ke PKBM lain di wilayah Banten guna menciptakan ekosistem digital suburban yang aman secara kolektif (Smith & Jones, 2021).

KESIMPULAN

Pelaksanaan program pengabdian kepada masyarakat berupa pelatihan keamanan data bagi warga belajar Paket C di PKBM Kampoeng Ilmu Center terbukti berhasil memberikan dampak positif dalam meningkatkan kewaspadaan terhadap ancaman siber dan penipuan daring. Peningkatan pemahaman warga belajar terlihat nyata dari lonjakan skor rata-rata evaluasi awal (pre-test) sebesar 45% yang berhasil meningkat menjadi 88% pada evaluasi akhir (post-test). Seluruh peserta juga telah memiliki keterampilan praktis untuk memproteksi perangkat smartphone mereka secara mandiri

melalui pembuatan kata sandi mnemonik yang kuat serta pengaktifan fitur verifikasi dua langkah (2FA).

Integrasi nilai-nilai moral tabayyun sebagai pertahanan kognitif terhadap rekayasa sosial dan amanah sebagai komitmen melindungi kredensial data pribadi terbukti menjadi pendekatan yang sangat efektif dalam memperkuat literasi digital di lingkungan pendidikan nonformal. Diharapkan, model edukasi interaktif berbasis praktik langsung ini dapat dijadikan acuan oleh institusi pendidikan tinggi lainnya dalam menyelenggarakan kegiatan pengabdian masyarakat yang berkelanjutan guna membangun ketahanan siber berbasis komunitas di Indonesia.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Pamulang atas dukungan pendanaan yang diberikan untuk pelaksanaan kegiatan Pengabdian kepada Masyarakat (PKM) ini berdasarkan Kontrak Kegiatan Nomor: 0001/D5/SPKPM/LPPM/UNPAM/III/2026. Ucapan terima kasih juga disampaikan kepada Ketua Program Studi Sistem Informasi, Bapak Heri Haerudin, S.Kom., M.Kom., atas arahan dan dukungan administratifnya. Penulis juga mengapresiasi Bapak Fiqhi Farabi selaku Kepala Sekolah PKBM Kampoeng Ilmu Center yang telah bersedia memfasilitasi tempat dan waktu, seluruh rekan-rekan mahasiswa pendamping, serta warga belajar Paket C atas partisipasi aktif dan kerja samanya selama kegiatan berlangsung.

REFERENSI

Ahmadi, A., & Hermawan, D. (2021). Peran pendidikan kesetaraan dalam meningkatkan literasi digital masyarakat marginal di PKBM. Jurnal Pendidikan Nonformal, 16(2), 112-121.

Azkiya, A., Ichsan, M. B. P., Hasibuan, N. A. P. F., Andrianti, R., & Maulana, I. (2024). Analisis sistem autentikasi dua faktor (2FA) dalam meningkatkan keamanan akses. JIKUM: Jurnal Ilmu Komputer, 2(2), 85-94.

Farahanita, M., Setiawan, C. B., Sahtyawan, R., & Fatimah, N. (2022). Analisis kesadaran cyber security di kalangan pengguna layanan keuangan digital Indonesia. Teknomatika: Jurnal Informatika dan Komputer, 15(1), 33-42.

Hafidh, M. (2020). Reinterpretasi konsep tabayyun dalam etika komunikasi digital di era disrupsi informasi. Jurnal Studi Al-Qur'an, 16(1), 45-62.

Hartanto, B. D., Nugraha, T. A., Ramadhan, B. R., Pratama, M. A., & Alamsyah, R. P. (2024). Edukasi keamanan digital untuk meningkatkan kewaspadaan masyarakat terhadap link phishing. Jurnal Pengabdian Sosial, 3(2), 120-128.

Hidayat, R. (2022). Pembelajaran e-learning di PKBM: Tantangan infrastruktur dan kemampuan literasi warga belajar Paket C. Jurnal Kebijakan Pendidikan, 11(2), 143-152.

Kurniawan, R., & Saputra, A. (2022). Sosialisasi keamanan siber dan perlindungan data pribadi untuk generasi Z di wilayah suburban. Jurnal Pengabdian Sosial dan Humaniora, 1(3), 189-198.

Novitasari, U. (2025). Phishing berbasis AI sebagai serangan social engineering: Ancaman baru di dunia keamanan siber. Jurnal Ilmu Hukum, 14(2), 201-215.

Persada, P. (2021). Keamanan informasi dan faktor kelalaian manusia: Tinjauan sistematis. Jurnal Keamanan Siber Nasional, 5(2), 99-114.

Pratama, M. A., & Hartanto, B. D. (2023). Rancang bangun media edukasi interaktif berbasis web untuk pencegahan kejahatan siber di kalangan remaja. Jurnal Teknologi Informasi dan Edukasi, 10(2), 77-86.

Purba, O. W. (2018). Pengantar Keamanan Jaringan dan Literasi Digital. Penerbit Andi.

Ramadhan, A., & Fitriani, D. (2024). Phishing awareness among non-formal education students: An empirical study in Indonesia. International Journal of Cyber Education, 6(1), 45-56.

Sari, N. P., & Utami, R. D. (2021). Pengaruh sosialisasi keamanan informasi terhadap perilaku proteksi data pribadi pengguna smartphone. Jurnal Komunikasi dan Media, 8(2), 122-135.

Setyawan, A., & Wibowo, S. (2023). Pelatihan pembuatan password aman menggunakan teknik mnemonik untuk menghindari serangan brute force. Jurnal Pengabdian kepada Masyarakat (J-Dimas), 5(1), 12-20.

Smith, J., & Jones, M. (2021). Cyber hygiene practices in developing nations: Challenges and opportunities. Journal of Cyber Security Policy, 12(3), 301-318.

UNESCO. (2020). Digital Literacy Assessment Framework in Non-formal Education. UNESCO Publishing.

Wardhana, A. (2023). Integrasi nilai-nilai Islam dalam literasi teknologi informasi untuk menangkal radikalisme dan penipuan online. At-Ta'lim: Jurnal Pendidikan Islam, 22(1), 55-72.

Wijaya, H., & Kusuma, A. (2024). Evaluasi pre-test dan post-test dalam pelatihan literasi digital: Mengukur efektivitas intervensi edukasi. Jurnal Evaluasi Pendidikan, 15(1), 89-98.

Yasir, M., & Anwar, S. (2023). Etika bermedia sosial dan konsep tabayyun di kalangan remaja masjid: Pendekatan dakwah bil-hal. Jurnal Dakwah dan Komunikasi, 14(2), 210-224.

Yudistira, N., Lamba, E. F., Jauhari, R., Farhanna, F. R., & Palangan, C. Y. (2025). Penyuluhan keamanan informasi terkait ancaman phishing untuk meningkatkan literasi digital masyarakat. GIAT: Jurnal Teknologi untuk Masyarakat, 4(1), 45-53.