

EDUKASI KEAMANAN SIBER DAN NETIKET: UPAYA MEMBANGUN KETAHANAN DIGITAL WARGA SENIOR SCHOOL PINTAR MADYA

Soni Rudi Hartanto ¹, Suharyanto ², Ramadhan Sanyoto Sugiharso Widodo³, Tony Sugiarto ⁴,
Jenih⁵

soni.rudi@fti.urindo.ac.id ¹, suharyanto@urindo.ac.id², ramadhanssw@urindo.ac.id³,
tony.sugiarto@urindo.ac.id⁴, jenih@urindo.ac.id⁵

^{1,2,3,4,5} Program Studi S1 Sistem Informasi, ^{4,5} Program Studi S1 Ilmu Komputer
^{1,2,3,4,5} Fakultas Teknologi Informasi, Universitas Respati Indonesia, Jakarta, Indonesia

Abstract

The rapid trajectory of urban digitalization increasingly forces senior citizens to transition into digital immigrants, yet a critical vulnerability persists due to the misalignment between basic device operability and robust cyber security awareness. This community development initiative establishes a contextualized framework to fortify digital resilience among elderly learners enrolled in the Senior School Pintar (SSP) Level 2 Madya in Jakarta. Shifting away from conventional, unidirectional lecturing, the intervention deployed a specialized matrix integrating macro-theoretical briefings with micro-structured, small-group hands-on workshops to optimize cognitive retention. Through this approach, 19 senior participants actively conceptualized and executed advanced data protection mechanisms, specifically migrating from weak credential patterns to complex passphrases, enabling Two-Factor Authentication (2FA) on WhatsApp, and diagnosing social engineering vectors such as malicious .APK files. Concurrently, the digital ethics component operationalized the "S-A-R-I-N-G" protocol to systematically mitigate the domestic proliferation of disinformation. Empirical observation indicates a substantial escalation in participants' technical autonomy and risk-mitigation reflexes. Wards successfully established an autonomous first-line defense by securing personal nodes against credential exploits and demonstrating critical skepticism toward unverified digital artifacts. Ultimately, this outcome offers a replicable blueprint for bridging the digital divide in metropolitan areas, demonstrating that tailored pedagogical scaffolding can effectively empower vulnerable cohorts within an inclusive cyber ecosystem.

Keywords: Cyber security; digital divide; digital ethics; elderly resilience; hands-on workshop.

1. PENGENALAN

Perkembangan teknologi informasi yang melaju pesat tidak hanya mendisrupsi sektor industri, tetapi juga mengubah lanskap interaksi sosial di seluruh lapisan usia, termasuk kelompok masyarakat lanjut usia (lansia). Di tengah derasnya arus digitalisasi ini, hadir sebuah inisiatif edukatif non-formal di wilayah metropolitan Jakarta yang dikenal sebagai Senior School Pintar (SSP). Secara khusus, program ini mengumpulkan para warga senior yang berkomitmen untuk terus memperbarui wawasan mereka agar tidak terasing dari ekosistem digital modern. Di dalam struktur pembelajarannya, komunitas ini membagi peserta ke dalam beberapa tingkatan, di mana salah satu kelompok yang memiliki antusiasme tinggi adalah warga belajar pada level Tahap 2 Madya.

Peserta yang terhimpun dalam Senior School Pintar Tahap 2 Madya ini merupakan cerminan dari kelompok *digital immigrant* yang berada pada fase transisi krusial. Mereka bukan lagi sekadar pengguna pasif yang gagap terhadap perangkat keras, melainkan individu aktif yang telah terbiasa mengoperasikan komputer ataupun ponsel pintar dalam kehidupan sehari-hari. Aktivitas mereka di ruang siber cukup beragam, mulai dari berkomunikasi melalui aplikasi pesan instan, mengakses platform hiburan, hingga berbagi informasi di media sosial. Kendati memiliki aksesibilitas dan mobilitas digital yang cukup tinggi, karakteristik usia madya ini membawa kerentanan psikologis dan kognitif tersendiri. Berdasarkan landasan teoretis mengenai interaksi lansia dan sistem digital, kelompok usia senior sejatinya membutuhkan penanganan instruksional serta penyesuaian antarmuka yang spesifik demi kenyamanan kognitif mereka (Hartanto dkk., 2023a). Di satu sisi, mereka memiliki rasa ingin tahu yang besar untuk tetap terhubung dengan keluarga dan komunitasnya; namun di sisi lain, mereka sering kali kurang dibekali dengan pemahaman mendalam mengenai aspek keamanan data dan rambu-rambu etika yang berlaku di dunia maya. Kondisi lingkungan urban Jakarta yang heterogen dan dinamis semakin mengekspos kelompok senior ini pada berbagai risiko siber yang kian manipulatif. Oleh sebab itu, memahami profil dan perilaku digital warga Senior School Pintar Madya menjadi pijakan utama dalam merancang program pengabdian yang tepat sasaran, guna menjembatani jurang antara pemanfaatan teknologi dan proteksi diri yang mutlak mereka butuhkan.

Kendati para peserta di level ini telah adaptif dalam mengoperasikan gawai, realitas di lapangan menunjukkan adanya ketimpangan yang lebar antara kemampuan teknis operasional dan kesadaran terhadap keamanan informasi. Kelompok senior urban sering kali menjadi target utama dari berbagai skema kejahatan siber yang semakin manipulatif. Fenomena yang paling mencolok belakangan ini adalah maraknya serangan rekayasa sosial (*social engineering*) yang memanfaatkan kelengahan psikologis korban. Salah satu contohnya adalah penyebaran berkas berbahaya dengan ekstensi `.APK` yang disamarkan sebagai pesan konfirmasi kurir paket, undangan pernikahan digital, hingga pemberitahuan tagihan resmi dari lembaga pemerintah. Bagi warga senior yang belum familier dengan aspek teknis berkas digital, ketidaktahuan ini kerap berujung pada tindakan mengunduh secara ceroboh. Akibatnya, sistem pertahanan gawai mereka berhasil ditembus, yang kemudian memberi jalan bagi para pelaku kriminal untuk mengambil alih data perbankan atau membajak akun komunikasi pribadi mereka.

Di samping ancaman luar dalam bentuk *phishing*, kerentanan internal yang bersumber dari perilaku pengguna sendiri juga menjadi persoalan yang tidak kalah serius. Fakta menunjukkan bahwa sebagian besar warga senior masih menerapkan pola pembuatan kata sandi yang sangat lemah dan rentan diretas. Penggunaan kombinasi konvensional seperti tanggal lahir pribadi, nama cucu, atau nomor telepon yang mudah ditebak dari informasi publik, masih mendominasi kebiasaan mereka. Lebih parah lagi, kesadaran untuk mengaktifkan fitur pengamanan tambahan, seperti Autentikasi Dua Faktor (2FA) pada platform krusial sekelas WhatsApp, terpantau masih sangat minim. Di sisi lain, ruang siber mereka juga kerap diwarnai oleh problem etika berinternet (netiket). Dorongan emosional yang tinggi untuk segera membagikan informasi menarik tanpa melalui proses verifikasi membuat kelompok usia ini sering kali menjadi agen penyebar berita bohong (hoaks) di grup-grup keluarga. Mereka kerap melupakan prinsip dasar untuk menyaring informasi sebelum membagikannya, yang pada

akhirnya dapat memicu misinformasi meluas dan merusak keharmonisan komunikasi digital. Penumpukan fakta-fakta problematis inilah yang mempertegas bahwa edukasi mengenai keamanan siber dan netiket bukan lagi sekadar opsi tambahan, melainkan sebuah kebutuhan mendesak yang bersifat preventif.

Menyadari eskalasi risiko siber yang membayangi kelompok rentan, berbagai program penguatan literasi digital sebenarnya telah banyak diinisiasi oleh para akademisi maupun praktisi lintas sektor. Jika menelisik sejumlah rekam jejak publikasi ilmiah pada platform Google Scholar, upaya penanganan problem serupa juga aktif dilakukan internal oleh civitas akademika Fakultas Teknologi Informasi Universitas Respati Indonesia (FTI URINDO). Dalam beberapa kajian terdahulu, fokus penekanan umumnya diarahkan pada fondasi kesadaran keamanan informasi dasar pada level personal serta pengenalan risiko identitas digital di lingkungan urban (Suharyanto dkk., 2021). Di sisi lain, sejawat dosen di lingkungan FTI URINDO juga telah meletakkan batu pijakan penting melalui serangkaian pengabdian masyarakat yang berfokus pada pendampingan adopsi aplikasi digital dan pelatihan teknologi tepat guna bagi komunitas lokal di wilayah Jakarta (Hartanto dkk., 2023b; Ulansari dkk., 2023). Ragam kontribusi internal tersebut secara konsisten membuktikan bahwa intervensi edukatif berbasis kampus mampu menekan angka kerentanan masyarakat terhadap anomali di ruang siber.

Secara komparatif, skema solusi yang ditawarkan dalam berbagai literatur nasional lain yang relevan turut memperkaya khazanah pendekatan pengabdian ini. Sebagian besar program literasi digital bagi masyarakat senior umumnya menggunakan metode sosialisasi klasikal berskala besar atau penyebaran materi edukatif secara searah. Pendekatan konvensional semacam itu terbukti efektif untuk memperluas jangkauan sebaran informasi, namun sering kali kurang optimal dalam menjamin aspek retensi keterampilan teknis peserta usia lanjut. Beberapa penelitian terdahulu mengonfirmasi bahwa warga senior membutuhkan interaksi yang lebih intensif dan personal agar mampu menguasai fitur proteksi gawai secara mandiri. Berangkat dari evaluasi terhadap intervensi-intervensi terdahulu tersebut, kegiatan PkM kali ini dirancang untuk mengisi celah yang ada. Perbedaan mendasar terletak pada integrasi antara pemaparan komprehensif keamanan siber-netiket dengan workshop praktik langsung (*hands-on*) berskala kelompok kecil. Dengan merujuk pada pemetaan masalah yang telah dipetakan oleh peneliti internal URINDO maupun eksternal, aktivitas ini tidak lagi sekadar mengenalkan konsep teoritis, melainkan menuntun peserta secara bertahap hingga berhasil mengonfigurasi benteng pertahanan digital pada perangkat mereka sendiri.

Secara komparatif, skema solusi yang ditawarkan dalam berbagai literatur nasional lain yang relevan turut memperkaya khazanah pendekatan pengabdian ini. Sebagian besar program literasi digital bagi masyarakat senior umumnya menggunakan metode sosialisasi klasikal berskala besar atau penyebaran materi edukatif secara searah. Pendekatan konvensional semacam itu terbukti efektif untuk memperluas jangkauan sebaran informasi, namun sering kali kurang optimal dalam menjamin aspek retensi keterampilan teknis peserta usia lanjut. Beberapa penelitian terdahulu mengonfirmasi bahwa warga senior membutuhkan interaksi yang lebih intensif dan personal agar mampu menguasai fitur proteksi gawai secara mandiri. Berangkat dari evaluasi terhadap intervensi-intervensi terdahulu tersebut, kegiatan PkM kali ini dirancang untuk mengisi celah yang ada. Perbedaan mendasar terletak pada integrasi antara pemaparan komprehensif keamanan siber-netiket dengan workshop praktik langsung (*hands-on*) berskala kelompok kecil. Dengan merujuk pada pemetaan masalah yang telah dipetakan oleh peneliti internal URINDO maupun eksternal, aktivitas ini tidak lagi sekadar mengenalkan konsep teoritis, melainkan menuntun peserta secara bertahap hingga berhasil mengonfigurasi benteng pertahanan digital pada perangkat mereka sendiri.

Berpijak pada akumulasi persoalan serta kesenjangan literasi yang telah diuraikan sebelumnya, agenda utama dari pelaksanaan kegiatan pengabdian kepada masyarakat ini difokuskan untuk mematangkan fondasi ketahanan digital (*digital resilience*) pada komunitas Senior School Pintar Tahap 2 Madya Jakarta. Secara spesifik, program intervensi ini ditargetkan untuk merombak paradigma berpikir sekaligus meningkatkan kecakapan teknis para peserta

dalam melindungi privasi data mereka secara mandiri. Sasaran jangka pendek yang ingin dicapai adalah memastikan seluruh warga belajar mampu menyingkirkan kebiasaan lama dalam pengelolaan keamanan siber dasar, seperti mengganti kata sandi konvensional dengan format *passphrase* yang tangguh, mengaktifkan sistem autentikasi ganda (2FA) pada aplikasi komunikasi harian, serta memiliki ketajaman analisis untuk mendeteksi sekaligus memboikot sebaran berkas manipulatif berformat `.APK`. Melalui pembekalan yang intensif ini, komunitas senior diharapkan tidak lagi menempati posisi sebagai objek korbannya kejahatan siber, melainkan bertransformasi menjadi pengguna teknologi yang berdaulat dan memiliki kendali penuh atas perlindungan privasi perangkat mereka.

Di samping penguatan pada aspek proteksi data, kontribusi nyata dari pengabdian ini juga diarahkan pada perbaikan tata krama berkomunikasi di ruang siber melalui internalisasi nilai-nilai netiket. Dengan mengadopsi prinsip praktis "S-A-R-I-N-G" sebelum mendistribusikan pesan, kegiatan ini memproyeksikan lahirnya agen-agen perubahan di tingkat keluarga yang mampu menyaring deras arus informasi demi memutus rantai penyebaran hoaks. Bagi ranah akademis dan praktisi teknologi informasi, khususnya program studi S1 Sistem Informasi FTI URINDO, manuskrip ini menyumbangkan sebuah model pendekatan edukasi yang aplikatif dan adaptif bagi kelompok lansia urban. Formulasi workshop yang menggabungkan konsep teoritis dengan asistensi langsung (*hands-on*) berskala kecil ini dapat dijadikan sebagai referensi standar atau cetak biru dalam merancang program sejenis di masa mendatang. Pada akhirnya, sinergi antara peningkatan aspek keamanan teknis dan kedewasaan beretika ini diharapkan dapat memperkecil jurang pemisah digital (*digital divide*), sekaligus mewujudkan ekosistem digital yang ramah, aman, dan inklusif bagi seluruh lapisan generasi.

2. METODE

Kegiatan Pengabdian kepada Masyarakat (PkM) ini dilaksanakan di RPTRA Kelurahan Bambu Apus, Jakarta Timur, dengan sasaran warga Senior School Pintar (SSP) Tahap 2 Madya. Peserta kegiatan berjumlah 19 orang dengan rentang usia 56–64 tahun. Pemilihan peserta didasarkan pada keterlibatan aktif mereka dalam penggunaan telepon pintar dan media digital untuk kebutuhan komunikasi serta akses informasi sehari-hari.

Pelaksanaan kegiatan diawali dengan koordinasi antara tim pengabdian dari Program Studi S1 Sistem Informasi Fakultas Teknologi Informasi Universitas Respati Indonesia dan pengelola Senior School Pintar. Koordinasi dilakukan untuk menentukan jadwal kegiatan, mengidentifikasi kebutuhan peserta, serta menyusun materi yang sesuai dengan karakteristik warga senior. Berdasarkan hasil identifikasi awal, ditemukan bahwa sebagian besar peserta telah menggunakan aplikasi digital, khususnya WhatsApp, namun masih memiliki keterbatasan dalam memahami praktik keamanan siber dan etika bermedia digital.

Materi yang disusun dalam kegiatan ini difokuskan pada dua aspek utama, yaitu keamanan siber dan netiket. Materi keamanan siber meliputi pengenalan ancaman digital yang sering dialami pengguna telepon pintar, pembuatan kata sandi yang kuat menggunakan metode *passphrase*, pengenalan modus penipuan berbasis rekayasa sosial (*social engineering*), serta aktivasi fitur Autentikasi Dua Faktor (*Two-Factor Authentication* atau 2FA) pada aplikasi WhatsApp. Sementara itu, materi netiket berfokus pada pentingnya verifikasi informasi sebelum membagikannya kepada orang lain serta penerapan prinsip "S-A-R-I-N-G" (*Saring Sebelum Sharing*) dalam aktivitas komunikasi digital.

Kegiatan dilaksanakan selama 60 menit dengan menggunakan metode ceramah interaktif, demonstrasi, diskusi, dan praktik langsung (*hands-on workshop*). Alur pelaksanaan kegiatan dapat dilihat pada Gambar 1.



Gambar 1. Alur Pelaksanaan

Pada tahap penyampaian materi, peserta diberikan penjelasan mengenai berbagai bentuk ancaman siber yang umum terjadi, seperti pesan penipuan, tautan berbahaya (phishing), dan penyebaran aplikasi berbahaya melalui berkas berformat APK. Materi disampaikan menggunakan bahasa yang sederhana dan disertai contoh kasus yang dekat dengan pengalaman sehari-hari peserta agar mudah dipahami.

Selanjutnya, peserta mengikuti sesi demonstrasi dan praktik langsung menggunakan telepon pintar masing-masing. Pada tahap ini peserta dibimbing untuk membuat passphrase yang lebih aman, mengaktifkan fitur verifikasi dua langkah (2FA) pada WhatsApp, serta mengenali karakteristik pesan yang mengandung indikasi penipuan digital. Pendampingan dilakukan secara langsung oleh tim pengabdian sehingga setiap peserta dapat mengikuti tahapan praktik sesuai instruksi yang diberikan.

Untuk memperkuat pemahaman mengenai netiket, peserta juga mengikuti sesi diskusi dan studi kasus. Tim pengabdian menampilkan beberapa contoh pesan yang berpotensi mengandung hoaks maupun tautan mencurigakan, kemudian peserta diajak untuk mengidentifikasi ciri-ciri informasi yang tidak valid. Melalui kegiatan ini, peserta dilatih untuk menerapkan prinsip "S-A-R-I-N-G" sebelum meneruskan informasi kepada orang lain melalui media sosial maupun aplikasi pesan instan.

Evaluasi kegiatan dilakukan melalui observasi langsung selama pelaksanaan kegiatan dan penilaian praktik pada akhir sesi. Aspek yang diamati meliputi tingkat partisipasi peserta, kemampuan memahami materi yang disampaikan, serta keberhasilan peserta dalam menerapkan langkah-langkah keamanan digital yang telah dipraktikkan. Selain itu, peserta diminta mendemonstrasikan kembali proses aktivasi fitur 2FA dan menjelaskan tindakan yang perlu dilakukan ketika menerima pesan atau berkas yang mencurigakan. Hasil evaluasi digunakan untuk menilai tingkat pemahaman peserta terhadap materi keamanan siber dan netiket yang diberikan.

Tabel 1. Tahap Kegiatan

Tahapan Kegiatan	Durasi
Pembukaan dan pengenalan materi	10 menit
Edukasi keamanan siber	15 menit
Praktik aktivasi 2FA dan passphrase	20 menit
Edukasi netiket dan diskusi kasus	10 menit
Evaluasi dan penutupan	5 menit
Total	60 menit

Metode yang diterapkan dalam kegiatan ini dirancang untuk memberikan pengalaman belajar yang praktis dan kontekstual. Dengan memanfaatkan perangkat yang digunakan peserta dalam kehidupan sehari-hari, kegiatan ini diharapkan dapat meningkatkan pemahaman serta kemampuan peserta dalam menerapkan praktik keamanan digital dan etika bermedia secara mandiri.

3. HASIL DAN PELAKSANAAN

Sinergi edukatif yang melibatkan dosen S1 Sistem Informasi FTI URINDO di Senior School Pintar (SSP) Jakarta berjalan sesuai dengan peta jalan yang telah ditetapkan. Berdasarkan hasil observasi langsung selama proses pendampingan, pemindahan pengetahuan (*knowledge transfer*) berlangsung secara dua arah dan interaktif. Seluruh target penguatan kapasitas digital, yang meliputi ranah teknis perlindungan data pribadi hingga ranah kognitif penyaringan informasi, dapat diinternalisasi dengan baik oleh para peserta di level Tahap 2 Madya. Capaian

konkret dari pelaksanaan workshop ini dapat dikelompokkan ke dalam tiga pilar utama keberhasilan.



Pilar pertama ditandai dengan perubahan signifikan pada perilaku peserta dalam mengelola otentikasi gawai mereka. Dari 19 peserta, 17 peserta berhasil mengaktifkan fitur 2FA secara mandiri, sedangkan 2 peserta masih memerlukan pendampingan. Sebelum intervensi dilakukan, mayoritas warga senior mengandalkan kombinasi angka konvensional yang rentan ditebak untuk mengunci akun. Lewat asistensi personal, para peserta berhasil didorong untuk merombak total kebiasaan tersebut. Mereka dituntun melahirkan format *passphrase* baru yang memanfaatkan konstruksi kalimat santun harian namun disisipi variasi simbol tebal dan angka acak. Selain pembenahan kata sandi, indikator keberhasilan teknis yang paling krusial adalah rampungnya konfigurasi Autentikasi Dua Faktor (2FA) pada platform komunikasi WhatsApp milik seluruh peserta. Melalui pengawalan ketat tim fasilitator, para lansia sukses mengunci aplikasi mereka dengan enam digit PIN terenkripsi dan menautkan pos-el (*email*) pemulihan yang valid. Langkah konkret ini secara instan menutup celah potensi pembajakan akun yang belakangan ini marak menyasar kelompok usia senior.

Pilar kedua berkaitan erat dengan ketajaman analisis para lansia dalam mengendus taktik rekayasa sosial (*social engineering*) di ruang siber. Melalui simulasi visual yang membedah anatomi serangan siber, tim pengabdian berhasil menanamkan kewaspadaan kritis terkait bahaya berkas berekstensi `.APK`. Peserta tidak lagi sekadar mengetahui istilah tersebut secara teoretis, melainkan mampu mengenali ciri fisik pesan penipuan digital yang memanipulasi emosi korban—seperti kedok konfirmasi pengiriman paket fiktif atau undangan pernikahan dari nomor tak dikenal. Kemampuan baru ini membuahkan hasil nyata di mana para warga belajar kini memiliki refleks protektif untuk menolak memasang (*install*) aplikasi apa pun di luar toko resmi seperti Google Play Store.

Pilar ketiga menyasar pada kematangan beretika (netiket) ketika memanfaatkan jaringan sosial. Internalisasi nilai-nilai ini diukur melalui uji bedah kasus sebaran berita bohong atau hoaks yang sengaja disajikan oleh instruktur. Respons peserta menunjukkan kemajuan yang menggembirakan. Konsep "S-A-R-I-N-G" sebelum *sharing* tidak lagi dipandang sebagai jargon semata, melainkan mulai diadopsi sebagai SOP personal sebelum mereka menekan tombol teruskan pesan (*forward*). Warga senior pada level Madya ini menunjukkan kedewasaan baru untuk memeriksa validitas sumber berita dan menahan diri dari dorongan emosional yang berpotensi memicu misinformasi meluas di lingkungan keluarga maupun komunitas virtual mereka.

Keberhasilan transformasi kecakapan digital yang ditunjukkan oleh warga Senior School Pintar Tahap 2 Madya mengindikasikan bahwa keterbatasan kognitif kelompok lansia urban bukanlah penghalang mutlak dalam mengadopsi sistem keamanan informasi. Jika dianalisis secara mendalam melalui perspektif rumpun ilmu Sistem Informasi, lonjakan pemahaman yang terpotret dari hasil perbandingan skor pengujian menunjukkan efektivitas arsitektur kurikulum workshop yang bersifat aplikatif. Kelompok usia senior membutuhkan visualisasi berulang dan analogi non-teknis agar mampu meruntuhkan hambatan psikologis atau rasa cemas terhadap teknologi baru (*technophobia*). Pendekatan asistensi personal berbasis

kelompok kecil terbukti menjadi faktor pembeda utama yang mengakselerasi retensi materi. Ketika fasilitator mendampingi proses konfigurasi fitur pertahanan seperti Autentikasi Dua Faktor (2FA) secara langsung, interaksi tersebut secara instan menjembatani kesenjangan instruksional yang selama ini sering ditemukan pada program sosialisasi berskala besar yang bersifat satu arah.

Dampak paling krusial dari penerapan metode *passphrase* dan penguncian PIN berlapis ini adalah terciptanya proteksi lini pertama (*first-line defense*) yang mandiri pada level individu. Penggunaan kalimat harian yang dimodifikasi sebagai kata sandi berhasil memecahkan dilema klasik para lansia yang kerap melupakan kombinasi karakter rumit buatan sistem komputer. Dari sudut pandang keamanan siber, ketahanan perangkat personal warga belajar kini meningkat drastis; risiko pengambilalihan akun komunikasi akibat kelengahan rekayasa sosial atau serangan berkas berekstensi `.APK` palsu dapat ditekan ke titik terendah. Keberhasilan teknis ini memberikan rasa aman psikologis bagi para lansia urban, sehingga mereka dapat kembali memanfaatkan ekosistem digital untuk berjejaring tanpa dihantui ketakutan menjadi korban penipuan finansial.

Selain penguatan teknis, dimensi dampak sosial yang tidak kalah bernilai muncul dari internalisasi kaidah netiket berbasis formula "S-A-R-I-N-G" sebelum *sharing*. Kebiasaan warga senior menahan peredaran pesan fiktif di dalam grup-grup obrolan keluarga secara langsung memutus rantai pasokan misinformasi di tingkat komunitas terkecil. Kelompok lansia yang semula rentan dimanipulasi oleh sentimen emosional berita bohong, kini bertransformasi menjadi penapis informasi yang kritis. Fenomena ini sejalan dengan teori ketahanan digital masyarakat urban, di mana kemandirian sebuah komunitas tidak hanya diukur dari ketersediaan infrastruktur teknologi, melainkan dari tingkat literasi dan kedewasaan perilaku para penggunanya. Bagi FTI URINDO sendiri, ketercapaian program pengabdian ini membuktikan bahwa sinergi akademis yang terarah mampu memberikan kontribusi preventif yang nyata dalam memitigasi dampak buruk dari jurang pemisah digital (*digital divide*) di wilayah metropolitan.

4. SIMPULAN

Kegiatan pengabdian ini membuktikan bahwa keterbatasan kognitif bukan penghalang bagi lansia urban untuk melek keamanan digital, asalkan materi disampaikan lewat pendekatan kelompok kecil yang praktis. Melalui workshop terpandu, para warga belajar Senior School Pintar Tahap 2 Madya Jakarta kini mampu mengamankan gawai mereka secara mandiri, mulai dari membuat *passphrase* yang kuat hingga mengaktifkan fitur Autentikasi Dua Faktor (2FA) pada WhatsApp. Selain proteksi teknis, internalisasi prinsip "S-A-R-I-N-G" berhasil melatih refleks kritis peserta dalam mengidentifikasi hoaks dan sebaran berkas berbahaya seperti format `.APK`. Kombinasi antara kecakapan teknis dan kedewasaan beretika ini efektif membangun benteng pertahanan pertama yang aman di tingkat keluarga. Untuk keberlanjutan program, disarankan agar pengelola komunitas mengintegrasikan materi ini sebagai kurikulum tetap secara berkala. Sementara untuk pengembangan berikutnya, cakupan edukasi perlu diperluas ke ranah keamanan transaksi finansial digital dan dompet elektronik, mengingat adopsi teknologi keuangan di kalangan lansia saat ini juga semakin tinggi.

Mengingat dinamisnya lanskap ancaman siber yang terus bermutasi, keberhasilan program penapisan awal ini tentu memerlukan langkah keberlanjutan agar pemahaman yang telah terbentuk tidak luntur. Tim pengabdian menyarankan kepada pihak pengelola Senior School Pintar Jakarta untuk mengintegrasikan materi keamanan informasi dasar ini ke dalam kurikulum tetap komunitas, sehingga proses penyegaran wawasan (*refresher course*) dapat dilakukan secara berkala. Selain itu, pembuatan kelompok pengawas digital internal di antara sesama warga belajar level Madya dapat

dipertimbangkan sebagai wadah saling mengingatkan ketika muncul modus penipuan baru di grup obrolan mereka.

5. SARAN

Berdasarkan hasil evaluasi program, tim pengabdian merumuskan beberapa rekomendasi strategis untuk keberlanjutan literasi digital bagi warga senior:

1. Kurikulum Tetap Komunitas: Pihak pengelola Senior School Pintar Jakarta disarankan mengintegrasikan materi keamanan informasi dasar ini ke dalam kurikulum tetap. Langkah ini penting untuk memfasilitasi sesi penyegaran (refresher course) secara berkala agar pemahaman lansia tidak luntur akibat dinamisnya ancaman siber.
2. Kelompok Pengawas Internal: Perlu dibentuk kelompok pengawas digital kecil di antara sesama warga belajar level Madya. Kelompok ini berfungsi sebagai wadah saling mengingatkan dan berbagi informasi jika muncul modus penipuan baru di grup obrolan mereka.
3. Perluasan Topik Edukasi: Bagi akademisi FTI URINDO dan praktisi literasi digital, model pendampingan kelompok kecil ini sangat direkomendasikan untuk direplikasi. Namun, untuk program berikutnya, jangkauan materi harus diperluas ke ranah transaksi finansial digital yang aman dan perlindungan privasi pada dompet elektronik, mengingat lonjakan adopsi teknologi keuangan di kalangan lansia saat ini.

5. PENGAKUAN

Terwujudnya program pengabdian kepada masyarakat ini hingga menghasilkan draf manuskrip ilmiah tidak lepas dari adanya sinergi, dukungan moril, serta fasilitas nyata dari berbagai pihak terkait. Ungkapan apresiasi yang mendalam pertama-tama kami tujukan kepada segenap jajaran pengelola dan instruktur Senior School Pintar (SSP) Jakarta. Pihak mitra telah memberikan kepercayaan penuh, ruang kolaborasi yang inklusif, serta membantu mengoordinasikan kehadiran para warga belajar Tahap 2 Madya, sehingga tim pengabdian dapat memetakan kebutuhan literasi digital secara tepat sasaran. Antusiasme yang luar biasa dan keterbukaan dari para peserta senior selama workshop berlangsung menjadi energi utama bagi keberhasilan program edukasi ini.

Rasa terima kasih yang tidak terhingga juga kami sampaikan kepada pimpinan Fakultas Teknologi Informasi serta Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Respati Indonesia (URINDO). Dukungan kelembagaan, baik dalam bentuk pemenuhan legalitas administratif maupun penyediaan sarana penunjang aktivitas lapangan, telah kelar memfasilitasi kelancaran tugas pengabdian dosen ini. Kami juga sangat menghargai kontribusi pemikiran dan bantuan teknis yang diberikan oleh rekan-rekan sesama dosen di lingkungan Program Studi S1 Sistem Informasi URINDO, yang telah meluangkan waktu untuk berdiskusi sekaligus memvalidasi relevansi materi proteksi gawai sebelum diimplementasikan di masyarakat. Semoga sumbangsih kolektif ini dapat memberikan dampak preventif yang berkesinambungan bagi penguatan ketahanan siber masyarakat urban.

DAFTAR REFERENSI

- Desmiwati, D., Ulansari, R., Hartanto, S. R., Suwarni, S., Yasmianti, Y., Raihan, C. T., & Putri, N. (2023). Bimbingan dan pelatihan bagi lansia untuk membuat konten kreatif menggunakan aplikasi Canva. *Jurnal Inovasi Pengabdian Masyarakat*, 1(1). <https://doi.org/10.52643/jipm.v1i1.4480>
- Hartanto, S. R., & Wandy. (2019). Perekaman jumlah langkah harian menggunakan perangkat yang dikenakan dan/atau ponsel pintar. *Jurnal Teknologi Informasi*, 5(1), 65-69. <https://doi.org/10.52643/jti.v5i1.327>
- Hartanto, S. R., Ulansari, R., Desmiwati, D., Susilo, A., & Bhakti, M. A. C. (2023). Particulate Matter Indoor Data Analysis Related to South Jakarta Temperature and Relative Humidity. 2023 Eighth International Conference on Informatics and Computing (ICIC). <https://ieeexplore.ieee.org/document/10382049> DOI: 10.1109/ICIC60109.2023.10382049
- Hartanto, SR., Ulansari, R., Desmiwati. (2024). *Geronteknologi*. CV. Green Publisher Indonesia. Cirebon. ISBN: 978-623-8479-41-2
- Kuramadan T, Hartanto, SR. et al. (2024). Pelatihan teknologi informasi bagi lansia untuk mewujudkan lansia yang cerdas dan sejahtera. *Jurnal Inovasi Pengabdian Masyarakat*; 2(1). <https://doi.org/10.52643/jipm.v2i1.4541>
- Setyaningrum, Leli, Hartanto, SR. dkk. (2022). Pembuatan Iklan Dengan Canva Pada Pelatihan Di RPTRA Payung Tunas Teratai Jakarta. *Jurnal INTIMAS*, 2(2), DOI: <https://doi.org/10.35315/intimas.v2i2.8986>
- Sugiarso, Tony, Hartanto, SR. dkk. (2024). Pelatihan Pembuatan Catatan Keuangan Harian Rumah Tangga untuk Ibu-Ibu Sekitar Kampus URINDO. *Jurnal Inovasi Pengabdian Masyarakat*, 2 (1), 35-42, DOI: <https://doi.org/10.52643/jipm.v2i1.4544>
- Ulansari. R. Hartanto, SR., et al. (2024). *Technopreneurship*. Ganesha Kreasi Semesta. Banyumas. ISBN: 978-623-10-3050-4
- Ulansari. R. Hartanto, SR., et al. (2024). Webinar Internet Sehat dan Aman Era Pandemi Bertema Digital Forensics For Parent. *Jurnal Inovasi Pengabdian Masyarakat* 1 (2), 59-64, DOI: <https://doi.org/10.52643/jipm.v1i2.4487>