BHINNEKA PUBLISHING

JURNAL PENGABDIAN MASYARAKAT BHINNEKA
Volume 4, No. 2, Tahun 2025
https://bhinnekapublishing.com/ojsbp/index.php/Jpmb

***e-ISSN** : 2963-3753*

Cyber Safety for All : Edukasi Keamanan Digital bagi Peserta *Fun Run*

Hendro Zalmadani[1], Muhammad Fakhri Rahmat Muzakki[2], Prasetyaningsih[3], Nofri Zayani[4]
[1,2,3,4] *STIKes Piala Sakti Pariaman, Indonesia*

Received : 25 November 2025, Revised : 1 Desember 2025, Published : 10 Desember 2025

Corresponding Author
Nama Penulis: Hendro Zalmadani
E-mail: hendro.zalmadani@gmail.com

Abstrak

Penggunaan internet di Indonesia yang mencapai lebih dari 221 juta pengguna meningkatkan risiko ancaman siber seperti pelanggaran data dan phishing, sementara literasi keamanan digital masyarakat masih rendah meskipun regulasi seperti UU PDP sudah diterapkan. Program pengabdian "Cyber Safety for All" bertujuan meningkatkan kesadaran dan keterampilan keamanan digital peserta Fun Run melalui pendekatan partisipatif-edukatif. Kegiatan dilaksanakan melalui empat tahap: persiapan, edukasi inti, pendampingan praktik, dan evaluasi. Pada tahap persiapan dilakukan analisis kebutuhan, penyusunan materi visual, dan koordinasi dengan panitia. Pelaksanaan mencakup mini workshop serta booth edukasi yang menyediakan konsultasi, pemeriksaan keamanan akun, dan demonstrasi langkah proteksi digital. Evaluasi pretest–posttest menunjukkan peningkatan pengetahuan peserta, terutama terkait phishing (56%), aplikasi berbahaya (42%), privasi lokasi (62%), dan dasar hukum keamanan digital (67%). Dari 200 peserta, 111 memiliki literasi digital rendah, menunjukkan tingginya kebutuhan edukasi pada komunitas olahraga yang aktif secara digital. Booth edukasi dikunjungi 135 peserta, dan 98 di antaranya mempraktikkan langsung penguatan keamanan akun. Program ini terbukti efektif meningkatkan kesadaran dan perilaku aman digital. Saran kami, untuk seterusnya edukasi serupa perlu diperluas dengan dukungan modul online, pembaruan materi, dan kolaborasi lintas sektor agar dampaknya berkelanjutan.
Kata Kunci - *cyber, digital, fun run*

Abstract

Indonesia's internet usage has surpassed 221 million users, increasing the risk of cyber threats such as data breaches and phishing. However, digital security literacy remains low despite the implementation of regulations like the PDP Law. The "Cyber Safety for All" community service program aims to enhance digital security awareness and skills among Fun Run participants through a participatory and educational approach. The program was conducted in four stages: preparation, core education, practical mentoring, and evaluation. During the preparation phase, needs analysis, development of visual materials, and coordination with the organizing committee were carried out. The implementation phase included mini-workshops and educational booths offering consultations, account security checks, and demonstrations of digital protection measures. Pretest-posttest evaluations revealed significant increases in participant knowledge, particularly regarding phishing (56%), malicious applications (42%), location privacy (62%), and the legal basis for digital security (67%). Among the 200 participants, 111 exhibited low digital literacy, highlighting a strong need for education within the digitally active sports community. The educational booth was visited by 135 participants, with 98 actively practicing account security strengthening measures. This program has proven effective in raising digital security awareness and promoting safer behaviors. We recommend expanding similar educational programs with the support of online modules, regularly updated materials, and cross-sector collaboration to ensure sustainable impact.
Keywords - *cyber, digital, fun run*

How To Cite : *Zalmadani, H., Muzakki, M. F. R., Prasetyaningsih, P., & Zayani, N. (2025). Cyber Safety for All: Edukasi Keamanan Digital bagi Peserta Fun Run. Jurnal Pengabdian Masyarakat Bhinneka, 4(2), 2547 - 2554. https://doi.org/10.58266/jpmb.v4i2.811*

PENDAHULUAN

Perkembangan pesat penggunaan internet di Indonesia telah menjadikan ranah digital sebagai bagian tidak terpisahkan dari kehidupan sehari-hari masyarakat. Menurut laporan CSIRT-BSSN, pada tahun 2024 jumlah pengguna internet di Indonesia tercatat mencapai 221,56 juta jiwa, dengan penetrasi internet mencapai 79,5 % dari populasi (Salwa, 2024). Angka ini menunjukkan bahwa sebagian besar warga kini aktif *online*, yang berdampak langsung pada tingginya volume data pribadi yang mengalir melalui aplikasi pendaftaran acara, media sosial, dan sistem pelacakan (*tracking*) digital. Dalam konteks penyelenggaraan acara publik seperti *fun run*, para peserta tidak hanya berinteraksi secara fisik tetapi juga menggunakan platform digital untuk mendaftar, berbagi dokumentasi, melacak rute lari, dan menautkan pengalaman mereka di media sosial. Kehadiran teknologi ini menghadirkan kemudahan, tetapi juga membuka celah risiko keamanan digital yang signifikan.

Risiko tersebut semakin diperparah oleh realitas bahwa ancaman siber di Indonesia yang terus meningkat. Laporan "Lanskap Keamanan Siber Indonesia 2023" dari BSSN mencatat total 403,99 juta anomali trafik sepanjang tahun, termasuk 4.001.905 aktivitas *Advanced Persistent Threat* (APT) dan lebih dari satu juta insiden *ransomware*. Berdasarkan laporan tersebut juga ditemukan dugaan 347 insiden siber, dengan jenis insiden terbanyak adalah pelanggaran data (*data breach*), dan ditemukan lebih dari 1,6 juta temuan *eksposur* data di *darknet* yang berdampak pada ratusan *stakeholder* (BSSN, 2024). Ancaman demikian menunjukkan bahwa data pribadi di Indonesia tidak hanya rentan disalahgunakan, tetapi eksposurnya bisa meluas, bahkan berakhir di ruang bawah tanah dunia maya.

Di tengah tingginya risiko, literasi keamanan digital di masyarakat Indonesia masih tergolong rendah. Menurut juru bicara BSSN yaitu Bapak Ariandi Putra bahwa pilar keamanan digital dalam indeks literasi digital secara konsisten menjadi yang paling rendah dibanding pilar lain seperti etika digital dan budaya digital. Menurut survei Katadata-Kominfopada tahun 2022, skor literasi pilar *Digital Safety* hanya 3.18 untuk laki-laki dan 3.07 untuk perempuan (skala 1-5), lebih rendah dibanding pilar etika dan budaya digital. Ini menandakan kesenjangan signifikan antara penggunaan internet yang masif dengan pemahaman keamanan digital yang mendalam di masyarakat. Selain itu, tercatat indeks literasi digital nasional telah meningkat, tetapi pilar keamanan digital masih memerlukan perhatian serius (Kominfo, 2022)

BSSN juga telah meluncurkan kampanye literasi keamanan siber bernama "Siap Jaga Ruang Siber", yang mengedepankan pesan sederhana seperti "Simpan datamu, Ikuti literasi, Amankan gadgetmu, Perkuat passwordmu (SIAP)". Namun masih banyak kelompok masyarakat yang belum menjangkau edukasi tersebut, terutama dalam konteks peristiwa publik atau komunitas olahraga. Dari sisi regulasi, landasan hukum terkait keamanan data juga semakin diperkuat. Indonesia telah mengesahkan Undang-Undang Perlindungan Data Pribadi (UU PDP) tahun 2022, yang mensyaratkan keamanan pemrosesan data dari pengaksesan yang tidak sah, pengungkapan yang tidak sah dan penyalahgunaan. Selain itu, UU ITE dan peraturan penyelenggaraan sistem elektronik mewajibkan penyelenggara sistem untuk menjaga keamanan sistem elektronik agar dapat diandalkan.

Di sisi sosial, meskipun regulasi telah tersedia, pemantauan publik terhadap implementasi UU PDP masih sangat dibutuhkan. Lembaga seperti *SAFEnet* mencatat ratusan kebocoran data pribadi dalam dua tahun terakhir, termasuk data pemilih yang sangat sensitif, dan mendorong keterlibatan publik untuk mengawasi pelaksanaan regulasi perlindungan data pribadi (SAFEnet, 2024). Kondisi ini menunjukkan bahwa regulasi tanpa literasi yang memadai dan partisipasi masyarakat berisiko menjadi kurang efektif dalam melindungi individu dari eksposur data.

Oleh karena itu, sangat diperlukan partisipasi masyarakat dalam menjaga dari penyalahgunaan data melalui literasi digital yang baik. Berdasarkan pengalaman pengabdian dan penelitian sebelumnya, literasi digital telah terbukti berdampak positif. Studi pilot oleh Thomas et al., (2021) menunjukkan bahwa program literasi media *daring* (*online*) dapat mengurangi kecenderungan mempercayai berita palsu *(fake news*) di antara pengguna internet Indonesia. Temuan ini relevan karena literasi semacam

ini selain menangkal hoaks, juga melatih sikap kritis yang penting untuk mengidentifikasi potensi serangan *phishing*, tautan berbahaya, dan modus digital lainnya (Parulian dkk., 2024).

Realitas digital modern, maraknya ancaman siber, dan rendahnya literasi keamanan digital meskipun regulasi mulai diperkuat, memunculkan kebutuhan mendesak untuk intervensi yang kontekstual dan praktis. Salah satu pendekatan yang sangat relevan adalah melalui acara komunitas publik seperti *fun run*. *Event* semacam ini tidak hanya mengumpulkan partisipasi fisik, tetapi juga digital mulai dari pendaftaran *online*, foto, *check-in* lokasi, hingga berbagi pengalaman di media sosial. Oleh karena itu, pengabdian "*Cyber Safety for All*: Edukasi Keamanan Digital bagi Peserta *fun run*" dirancang sebagai program yang menyasar peserta *event* olahraga massal dengan edukasi praktis, ringan, tetapi berbasis hukum dan keamanan.

Tujuan umum dari kegiatan pengabdian ini adalah meningkatkan kesadaran dan keterampilan dasar keamanan digital di kalangan peserta *fun run* sehingga mereka memahami potensi risiko digital dan dapat mengambil tindakan proaktif untuk melindungi data pribadinya. Secara spesifik, pengabdian ini bertujuan untuk: (1) menyampaikan edukasi risiko digital umum seperti *phishing*, tautan palsu, dan pelanggaran data melalui mini-workshop, materi cetak (leaflet / infografis); (2) mengajarkan tindakan praktis yang bisa langsung diterapkan oleh peserta, misalnya memverifikasi tautan pendaftaran, mengatur privasi media sosial, memperkuat kata sandi, dan mengaktifkan autentikasi dua faktor; (3) mengembangkan *checklist* keamanan sederhana untuk penyelenggara *fun run* agar mereka dapat menerapkan prosedur minimal dalam pengumpulan, penyimpanan, dan penghapusan data peserta; (4) memfasilitasi mekanisme pelaporan insiden digital (misalnya *phishing*) yang mudah diakses peserta; dan (5) mengevaluasi dampak intervensi melalui survei singkat sebelum dan sesudah kegiatan guna mengukur perubahan pengetahuan dan niat perilaku peserta. Program ini diharapkan mampu menjembatani jurang antara penggunaan teknologi digital dalam event publik dan kesadaran hukum-keamanan yang masih rendah, sekaligus memperkuat penerapan regulasi yang ada seperti UU PDP dan UU ITE di ranah masyarakat sehari-hari.

METODE

Pelaksanaan kegiatan pengabdian masyarakat "*Cyber Safety for All*: Edukasi Keamanan Digital bagi Peserta *Fun Run*" menggunakan pendekatan partisipatif-edukatif, yang menekankan keterlibatan aktif peserta melalui penyampaian materi, demonstrasi, dan praktik langsung. Metode ini dipilih karena sesuai dengan karakteristik acara *Fun Run* yang bersifat publik, terbuka, dan melibatkan berbagai kelompok usia dengan tingkat literasi digital yang beragam. Secara garis besar, kegiatan dilaksanakan melalui empat tahapan utama yaitu persiapan, pelaksanaan edukasi inti, pendampingan praktik, dan evaluasi dampak program. Pada tahap persiapan, dilakukan analisis kebutuhan penysuunan materi, persiapan media dan peralatan, dan koordinasi dengan panitian *Fun Run.* Analisis kebutuhan dilakukan dengan mengidentifikasi kebutuhan keamanan digital yang relevan bagi peserta *Fun Run*, meliputi risiko *phishing* pada tautan pendaftaran, potensi kebocoran data pribadi, keamanan penggunaan aplikasi olahraga, privasi foto dan lokasi peserta.

Informasi yang didapatkan kemudian dihimpun melalui observasi awal proses registrasi *Fun Run*, analisis sistem informasi panitia, serta diskusi dengan penyelenggara acara. Selanjutnya, penyusunan materi edukasi dalam *Power Point Text* (PPT) yang ringkas, visual, dan mudah dipahami, berupa risiko *phishing* dan tautan palsu, cara mengenali aplikasi berbahaya, pentingnya menjaga privasi lokasi saat menggunakan aplikasi pelacak rute, aturan dasar keamanan digital sesuai UU ITE dan UU Perlindungan Data Pribadi. Materi ini disampaikan dalam waktu 20 menit. Persiapan alat yang digunakan yaitu leaflet, banner infografis, QR *code* berisi panduan lengkap, perangkat audio untuk penyampaian sesi edukasi, dan kuesioner online dengan *google form* untuk survei *pretest* dan *posttest*. Koordinasi dengan panitia dilakukan untuk menentukan lokasi *booth* edukasi, waktu penyampaian materi di panggung utama, dan mekanisme penyebaran QR code kepada peserta.

Tahap pelaksanaan dilaksanakan pada hari kegiatan *Fun Run* melalui beberapa metode terintegrasi yaitu mini *workshop* (10–20 menit) dan *booth* edukasi. Mini *workshop* dengan memberikan edukasi singkat di area panggung utama mengenai risiko *phishing* dan tautan palsu, cara mengenali aplikasi berbahaya, pentingnya menjaga privasi lokasi saat menggunakan aplikasi pelacak rute, aturan dasar keamanan digital sesuai UU ITE dan UU Perlindungan Data Pribadi dengan menggunakan PPT dan leaflet, dan *banner* infografis. *Booth* edukasi digunakan untuk konsultasi singkat mengenai keamanan akun pribadi, pemeriksaan kekuatan kata sandi, demonstrasi aktivasi autentikasi dua faktor,

penjelasan cara mengatur privasi foto dan lokasi di media sosial, dan pembagian leaflet dan QR panduan keamanan digital. Penyediaan *booth* edukasi untuk memberikan pendampingan langsung sehingga memastikan pemahaman yang lebih mendalam. Tahap evaluasi dilakukan untuk mengukur keefektivitasan kegiatan. Pada kegiatan ini, evaluasi dilakukan melalui kuisioner *pretest* dan *posttest,* serta antusias peserta yang dilihat dari jumlah daftar hadir mini *workshop* dan *booth* edukasi. Hasil evaluasi dijadikan dasar penyusunan artikel dan laporan akhir pengabdian serta rekomendasi penguatan keamanan digital pada *event* publik di masa mendatang.

HASIL DAN PEMBAHASAN

A. Hasil Kegiatan

Pelaksanaan kegiatan pengabdian masyarakat *Cyber Safety for All*: Edukasi Keamanan Digital bagi Peserta *Fun Run* menghasilkan sejumlah temuan penting terkait perubahan pengetahuan, sikap, serta kesiapan peserta *Fun Run* dalam memahami dan menerapkan praktik keamanan digital. Kegiatan yang terdiri dari pengisian kuisioner *pretest* dan *posttest,* mini-*workshop*, pembagian leaflet edukatif, dan *booth* edukasi ini diikuti oleh 200 peserta dari berbagai kelompok usia, terutama remaja dan dewasa muda. Secara umum, kegiatan berlangsung efektif dan mendapat respon positif dari peserta maupun penyelenggara acara.

Hasil pengetahuan *pretest* dan *posttest* dapat terlihat pada Tabel 1 berikut.

Tabel 1. tingkat pengetahuan peserta sebelum dan setelah diberikan edukasi

Indikator Pengetahuan	Pretest	*Posttest*	Peningkatan
	%	%	
Risiko *phishing* dan tautan palsu	23%	79%	56%
Keamanan digital dan pengenalan aplikasi berbahaya	41%	83%	42%
Pentingnya menjaga privasi lokasi saat menggunakan aplikasi pelacak rute	29%	91%	62%
Aturan dasar keamanan digital sesuai UU ITE dan UU Perlindungan Data Pribadi	7%	74%	67%

Berdasarkan pada Tabel 1 terlihat bahwa pengetahuan peserta mayoritas rendah pada berbagai indikator dan meningkat setelah diberikan edukasi. Peningkatan pengetahuan pada indikator risiko *phisihing* dan tautan palsu yaitu 56%, keamanan digital dan pengenalan aplikasi berbahaya 42%, pentingnya menjaga privasi lokasi saat menggunakan aplikasi pelacak rute (62%), dan aturan dasar keamanan digital sesuai UU ITE dan UU Perlindungan Data Pribadi (67%). Dari total 200 peserta yang ikut kegiatan ini, ada sebanyak 111 memiliki tingkat literasi keamanan digital peserta masih rendah. Temuan ini menegaskan bahwa komunitas olahraga seperti peserta *Fun Run*, merupakan kelompok yang sangat aktif secara digital tetapi belum memiliki pemahaman memadai mengenai keamanan data.

Peningkatan ini sejalan dengan hasil pengabdian oleh Eriana dkk (2023) yang menunjukkan bahwa edukasi keamanan digital berbasis komunitas *outdoor* dapat meningkatkan pengetahuan peserta sebesar 30–40%. Selain itu, Hartanto dkk (2025) juga menemukan bahwa pelatihan literasi digital berbasis masyarakat sangat efektif meningkatkan pemahaman dan kewaspadaan masyarakat terhadap risiko siber, terutama jika dikemas dalam bentuk praktik langsung seperti simulasi phishing atau analisis pesan berbahaya. Temuan kegiatan ini mendukung hasil-hasil kegiatan sebelumnya, terutama dalam konteks bahwa literasi keamanan digital menjadi lebih mudah dipahami ketika peserta dilibatkan dalam pengalaman yang aplikatif, singkat, dan sesuai konteks kehidupan sehari-hari. Pada akhir mini *workshop,* dilengkapi dengan simulasi *phisihing* sederhana. Menurut peserta, simulasi ini lebih nyata dalam menyadarkan peserta tentang bahanya data digital yang beredar sembarangan.

Kegiatan edukasi juga dilakukan di *Cyber Safety Booth* yang ditempatkan di area start/finish Fun Run. Peserta yang telah melakukan *fun run* diarahkan untuk mengunjungi *booth* sesudah berlari. Materi yang disampaikan meliputi tips melindungi data pribadi saat mengikuti event publik, cara mengidentifikasi tautan palsu dan phishing, pengaturan privasi media sosial sebelum unggah dokumentasi *Fun Run,* langkah aman menggunakan aplikasi pelacak lari (GPS *tracking*), dan panduan membuat kata sandi kuat dan penggunaan autentikasi dua faktor. Total 135 peserta tercatat berinteraksi langsung dengan *booth*. Sebanyak 98 peserta melakukan praktik langsung mengatur

keamanan akun, seperti aktivasi autentikasi dua faktor atau mengganti *password* lemah. Antusiasme pengunjung terlihat dari banyaknya peserta yang meminta demonstrasi langsung terkait *fake link detection* dan pengaturan privasi Instagram. Kegiatan ini dibantu juga oleh mahasiswa seperti dokumentasi yang terlihat pada foto 1 berikut.

Gambar 1. Foto bersama setelah acara

Selain pengetahuan, kegiatan ini juga meningkatkan kesadaran peserta mengenai pentingnya melindungi data pribadi. Sebelum pelatihan, hanya 27% peserta yang mengaktifkan fitur autentikasi dua faktor (2FA) pada akun media sosial atau email. Setelah kegiatan dan sesi konsultasi personal, jumlah tersebut meningkat menjadi 61%. Selain itu, terdapat perubahan sikap terkait perilaku berbagi informasi. Sebelum edukasi, sebanyak 72% peserta mengaku sering membagikan foto tiket atau *barcode* registrasi *Fun Run* ke Instagram atau WhatsApp tanpa menyadari risiko penyalahgunaan datanya. Setelah penyuluhan, sebagian besar peserta menyatakan tidak akan lagi membagikan data sensitif secara sembarangan.

Temuan ini menguatkan teori *Technology Threat Avoidance Theory* (TTAT) yang dikembangkan oleh Li (2014), yang menyatakan bahwa persepsi ancaman (*perceived threat*) dan persepsi efektivitas solusi (*perceived safeguard effectiveness*) merupakan faktor penentu utama perubahan perilaku keamanan digital. Ketika peserta memahami konsekuensi (risiko kebocoran data, akses akun oleh pihak tidak berwenang) dan mengetahui cara pencegahannya (2FA, verifikasi tautan, privasi akun), maka perilaku aman lebih mudah terbentuk.

B. Pembahasan

Temuan dari program kegiatan pengabdian masyarakat *Cyber Safety for All*: Edukasi Keamanan Digital bagi Peserta *Fun Run* memberikan gambaran nyata mengenai kondisi literasi keamanan digital masyarakat Indonesia di ruang-ruang publik nonformal. Program ini mengonfirmasi hasil temuan nasional yang sebelumnya telah dilaporkan oleh Katadata-Kominfo (2022), bahwa pilar *digital safety* merupakan aspek literasi digital dengan nilai paling rendah dibandingkan tiga pilar lainnya, yakni *digital culture, digital ethics,* dan *digital skills*. Rendahnya skor tersebut tampak selaras dengan perilaku peserta *Fun Run* yang aktif menggunakan media sosial namun tidak memahami risiko keamanan digital dalam aktivitas sehari-hari. Misalnya, banyak peserta dengan mudah membagikan foto tiket, *barcode* nomor peserta, serta lokasi *realtime* saat sedang berlari. Kebiasaan ini berpotensi membuka ruang eksploitasi, mulai dari pencurian identitas, *social engineering*, duplikasi *barcode*, hingga pelacakan lokasi yang dapat mengancam keamanan pribadi.

Salah satu temuan penting dari kegiatan ini adalah bahwa meskipun tingkat pemahaman awal peserta mengenai keamanan digital relatif rendah, respons mereka terhadap edukasi yang bersifat praktis dan kontekstual ternyata sangat positif. Ketika edukasi diberikan di tengah aktivitas komunitas yang santai seperti Fun Run, peserta tampak lebih antusias dan merasa bahwa materi tersebut relevan dengan pengalaman sehari-hari mereka. Hal ini memperkuat kesimpulan penelitian Saputra & Hidayat (2020) yang menegaskan bahwa model edukasi digital yang interaktif dan kontekstual jauh lebih efektif daripada metode ceramah tradisional, khususnya untuk kelompok masyarakat yang terbiasa dengan

lingkungan digital. Edukasi yang diberikan dengan bahasa sederhana, contoh nyata, dan langsung dikaitkan dengan kegiatan lari ternyata jauh lebih mudah diterima dan dipahami peserta.

Program ini juga menyertakan simulasi *phishing* sebagai bagian dari mini *workshop*. Bagian ini terbukti menjadi elemen paling menarik sekaligus paling efektif. Peserta diperlihatkan dua contoh pesan yaitu satu pesan resmi dari penyelenggara, dan satu lagi pesan palsu yang telah dimodifikasi untuk menyerupai pesan asli namun mengandung tautan berbahaya. Sebelum mengikuti simulasi, hasil *pretest* menunjukkan bahwa hanya 41% peserta yang mampu membedakan pesan *phishing* dari pesan asli. Namun, setelah mengikuti penjelasan, praktik langsung, dan diskusi kelompok kecil tentang ciri-ciri pesan palsu, angka tersebut meningkat drastis menjadi 88% pada *posttest*.

Peningkatan ini bukan hanya signifikan secara angka, tetapi juga menggambarkan perubahan pola pikir peserta dalam mengenali ancaman digital. Temuan tersebut sejalan dengan penelitian Thomas et al. (2021), yang menyatakan bahwa pelatihan literasi digital dengan pendekatan *hands-on* melalui simulasi, studi kasus, atau latihan langsung lebih efektif dalam meningkatkan ketahanan pengguna terhadap misinformasi dan serangan siber dibandingkan penyampaian informasi secara pasif. Kegiatan berbasis pengalaman seperti ini didukung oleh teori *experiential learning*, yang menjelaskan bahwa pembelajaran akan lebih bermakna ketika individu mengalami sendiri situasi yang relevan, menganalisisnya, dan kemudian mempraktikkan respons yang tepat.

Selain praktik langsung, salah satu aspek yang memperkuat keberhasilan program ini adalah penggunaan regulasi nasional sebagai dasar edukasi, yaitu Undang-Undang Perlindungan Data Pribadi (UU PDP, 2022) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Ketika fasilitator menjelaskan bahwa perlindungan data pribadi bukan hanya sekadar pilihan tetapi merupakan hak hukum yang dilindungi negara, peserta mulai memahami dimensi legal dari keamanan digital. Banyak peserta yang sebelumnya tidak mengetahui bahwa penyelenggara *Fun Run* maupun aplikasi olahraga wajib menerapkan standar keamanan tertentu untuk melindungi data pengguna. Setelah penjelasan tersebut, peserta menyatakan merasa lebih bertanggung jawab untuk menjaga datanya sendiri dan lebih kritis terhadap aplikasi yang meminta akses berlebihan.

Hasil kegiatan ini sejalan dengan laporan SAFEnet (2023) yang menunjukkan bahwa rendahnya kesadaran masyarakat terhadap hak-hak hukum terkait data pribadi menyebabkan masyarakat jarang menuntut akuntabilitas dari *platform* digital atau penyelenggara sistem elektronik. Dengan demikian, penggunaan landasan hukum dalam edukasi keamanan digital memberikan dua dampak sekaligus yaitu meningkatkan kesadaran individu mengenai pentingnya menjaga data pribadi, serta mendorong masyarakat untuk berpartisipasi dalam pengawasan implementasi regulasi.

Dari sisi sosial, program ini juga menyoroti bahwa tingginya interaksi digital dalam kegiatan *Fun Run* mulai dari pendaftaran *online*, pengambilan foto dengan kode QR, hingga berbagi aktivitas di media sosial membuat peserta sangat bergantung pada perangkat dan aplikasi digital. Namun, ketergantungan ini tidak diimbangi dengan kemampuan dasar untuk melindungi data pribadi. Oleh karena itu, program *Cyber Safety for All* hadir sebagai penghubung untuk menjembatani kesenjangan tersebut. Ketika peserta memahami bahwa hampir seluruh tindakan digital mereka meninggalkan jejak data, mereka menjadi lebih berhati-hati dalam berbagi informasi. Edukasi digital dapat menyelamatkan masyarakat dari penyalahgunaan teknologi digital (Karlina dkk, 2023; Zulfa, 2024; Wibowo & Hidayat, 2024).

Jika dibandingkan dengan kegiatan pengabdian masyarakat di bidang literasi digital lainnya, program ini memiliki kelebihan pada pendekatan praktis dan penyampaian materi di tengah aktivitas komunitas. Misalnya, penelitian Yudistira dkk (2025) dan Riandari dkk (2024) menunjukkan bahwa literasi dengan penyuluhan ditengah masyarakat hanya menumbuhkan kesadaran yang sementara tentang keamanan digital. Dananjoyo (2024) juga mengemukakan bahwa literasi digital pada masyarakat pedesaan juga hanya dapat meningkatkan pengetahuan tanpa disertai dengan kesadaran pentingnya keamanan digital. Hal ini bermakna bahwa penyampaian materi dengan penyajian yang menarik dapat meningkatkan keefektifan materi seperti melalui pemilihan atmosfer yang santai membuat peserta lebih terbuka dan aktif.

Selain itu, keberhasilan kegiatan ini juga dapat dijelaskan melalui pendekatan *behavioral change*. Edukasi keamanan digital tidak hanya menargetkan pengetahuan (*knowledge*), tetapi juga perubahan perilaku (*behavior*). Ketika peserta diajak bersama-sama mempraktikkan cara memverifikasi tautan, mengatur privasi media sosial, dan mengaktifkan autentikasi dua faktor, mereka tidak hanya menerima informasi, tetapi juga langsung menerapkannya. Hal ini sesuai dengan model perubahan

perilaku *Theory of Planned Behavior*, yang menyatakan bahwa niat perilaku meningkat ketika individu memiliki pengetahuan, pengalaman, serta keyakinan bahwa perilaku tersebut mudah dilakukan (Isa et al., 2022). Dalam konteks kegiatan ini, peserta menyatakan bahwa langkah-langkah keamanan digital ternyata tidak serumit yang mereka bayangkan.

Keseluruhan hasil program ini menunjukkan bahwa edukasi keamanan digital dapat dilakukan dengan efektif dalam ruang publik seperti event olahraga massal. Peserta tidak hanya mengalami peningkatan pengetahuan tetapi juga menunjukkan perubahan sikap dan niat untuk menjaga keamanan digital mereka. Temuan ini memperkuat pentingnya integrasi pendidikan cyber safety dalam berbagai kegiatan komunitas. Dengan demikian, kegiatan *Cyber Safety for All* bukan hanya edukasi sesaat, tetapi sebuah model intervensi yang dapat direplikasi pada *event-event* publik lainnya. Program ini menunjukkan bahwa ketika edukasi digital dirancang dengan metode yang tepat, interaktif, aplikatif, dan terhubung dengan konteks kegiatan agar masyarakat lebih mudah memahami ancaman siber serta lebih mampu melindungi data pribadi mereka.

KESIMPULAN DAN SARAN

Kegiatan pengabdian *Cyber Safety for All* terbukti efektif meningkatkan pengetahuan, kesadaran, dan perilaku aman peserta *Fun Run* terhadap keamanan digital melalui metode edukatif-interaktif, simulasi *phishing*, dan *booth* edukasi. Hasil ini menegaskan bahwa edukasi berbasis pengalaman nyata dan konteks komunitas mampu membentuk perilaku digital yang lebih aman. Disarankan untuk memperluas program edukasi keamanan digital di tengah masyarakat lain yang aktif secara digital serta memperkuat metode partisipatif seperti simulasi dan praktik langsung. Selain itu, tindak lanjut melalui modul *online*, pembaruan materi sesuai tren digital terbaru, dan kolaborasi lintas sektor dapat memastikan perubahan perilaku peserta tetap berkelanjutan.

UCAPAN TERIMA KASIH

Ucapan terima kasih kami ucapkan padaa Yayasan Piala Sakti Pariaman yang telah memberikan sumber pendanaan dan Pemerintah Kota Pariaman beserta panitia *Fun Run* Kota Pariaman yang telah memberikan izin pelaksanaan.

DAFTAR PUSTAKA

Isa, K., Hai Sam, T., Sarala Thulasi Palpanadan, A., & Vasudevan, A. (2022). Awareness of the Use of Social Media Among Students: Malaysia and Indonesia. *The Seybold Report*, *February 2024*, 83–94. https://doi.org/10.5281/zenodo.6955993.

Antara News. (2023). BSSN: Pilar keamanan digital masih rendah dalam literasi digital nasional. Diakses dari: https://www.antaranews.com

Badan Siber dan Sandi Negara. (2023). Lanskap Keamanan Siber Indonesia 2023. BSSN. diakses dari: https://bssn.go.id

CSIRT-BSSN. (2024). Statistik pengguna internet Indonesia 2024. diakses dari https://csirt.bssn.go.id

Databoks. (2022). Skor literasi digital Indonesia berdasarkan empat pilar. Katadata. diakses dari: https://databoks.katadata.co.id

Dananjoyo, S. W. (2024). Literasi digital di kalangan masyarakat pedesaan: Upaya meningkatkan kesadaran keamanan siber. *Jurnal Edutein: Edukasi dan Teknologi Informasi,* 2(1).

Eriana, E. S., Zein, A., Wati, F. E., & Buminata, M. S. A. (2023). Sosialisasi keamanan digital untuk mengatasi phishing dan apk berbahaya. *Attamkiim: Jurnal Pengabdian Masyarakat,* 2(1). https://doi.org/10.62070/attamkiim.v2i1.248

Hartanto, B. D., Nugraha, T. A., Ramadhan, B. R., Pratama, M. A., & Alamsyah, R. P. (2025). Edukasi keamanan digital untuk meningkatkan kewaspadaan masyarakat terhadap link phishing. *Jurnal Pengabdian Sosial,* 2(9), 4341–4346. https://doi.org/10.59837/nndaqp49.

Karlina K. Yustisia, Anis D. Winarsih, Malikhatul L. Lailiyah, Aditya N. Yudhawardhana, Anando S. Binatoro, & Qisthina Arifah. (2023). Edukasi literasi digital siswa sekolah dasar tentang strategi keamanan dan manajemen siber. *GERVASI: Jurnal Pengabdian kepada Masyarakat, 7*(1), 135–147. https://doi.org/10.31571/gervasi.v7i1.4472

Kementerian Informasi Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Jakarta: Sekretariat Negara.

Kementerian Informasi Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Jakarta: Sekretariat Negara.

Kominfo– Direktorat Jenderal Aplikasi Informatika. (2023). Laporan kinerja Direktorat Jenderal Aplikasi Informatika 2023. Kementerian Komunikasi dan Informatika RI. diakses dari: https://aptika.kominfo.go.id

Parulian Marpaung, A., Fadhillah, A., Ilhamsyah, H. R., Sya'roni, I. M., Ardiyanti, K. T., Renanda, M. F., & Muhajir, A. (2024). Sosialisasi dan edukasi terkait keamanan cyber security untuk generasi digital di SMP Islam Raudlatul Hikmah. A*PPA: Jurnal Pengabdian Kepada Masyarakat,* 2(5), 482–486.

Riandari, F., Tasril, V., & Ritonga, R. P. (2024). Increasing cybersecurity awareness among teenagers through digital education and simulation. *Abdimas*, 18(1)

SAFEnet. (2023). Laporan pemantauan kebocoran data di Indonesia 2021–2023. SAFEnet Indonesia. https://safenet.or.id

Saputra, R., & Hidayat, M. (2020). Social media risk awareness among youth: A cross-sectional study in Indonesia. *International Journal of Cyber Studies*, 4(2), 77–90.

Thomas, K., Hogan-Taylor, M., Yankoski, M., & Weninger, T. (2021). The impact of online media literacy training on misinformation beliefs among Indonesian internet users (arXiv:2106.12345). arXiv. diakses dari: https://arxiv.org/abs/2106.12345.

Wibowo, B., & Hidayat, T. (2024). Strategi efektif dalam meningkatkan kesadaran keamanan siber terhadap ancaman phishing di lingkungan perusahaan PT. XYZ: Simulasi phishing. *Jurnal Pengabdian Masyarakat Sultan Indonesia, 2*(1), 1–9. https://doi.org/10.58291/abdisultan.v2i1.294

Yudistira, N., Lamba, E. F., Jauhari, R., Farhanna, F. R., & Palangan, C. Y. (2025). Penyuluhan keamanan informasi terkait ancaman phishing untuk meningkatkan literasi digital warga Kompleks Yadara Babarsari Yogyakarta. *GIAT: Jurnal Teknologi untuk Masyarakat, 4*(1). https://doi.org/10.24002/giat.v4i1.11615

Zulfa Ar Rahman. (2024). Pemanfaatan teknologi informasi dalam edukasi literasi digital untuk peningkatan keamanan data dan pencegahan kejahatan siber di masyarakat Rawang Panca Arga. *Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika, 2*(6), 82–90. https://doi.org/10.61132/merkurius.v2i6.399