

PERAN STRATEGIS PEMERINTAH DAERAH DALAM MENINGKATKAN KESADARAN MASYARAKAT TERHADAP KEAMANAN SIBER

ANGGI ANGGRAENI KUSUMONINGTYAS¹, SELENTINUS GUNAWAN², RIZKIA RAMADHAN³, MU'MIN AZIZ⁴, DINAR PARADISA⁵

Program Studi Ilmu Pemerintahan, Universitas Pamulang^{1,2,3,4,5}

email: anggi.anggraeni@unpam.ac.id¹, selengunawan@gmail.com², paradisadinar55@gmail.com³, anna31aziez@gmail.com⁴, paradisadinar55@gmail.com⁵

Abstract: *This Community Service Program (PKM) titled "The Strategic Role of Local Government in Increasing Public Awareness of Cybersecurity" was carried out in Terumbu Village, Kasemen District, Serang City, Banten. The program aims to strengthen the role of local governments in educating the public about cybersecurity and improving the digital literacy of local government apparatus. Participatory lectures, cybercrime simulations, and group discussions were applied to enhance participants' understanding of cyber threats and prevention measures. Results indicate a significant increase in awareness, with local officers expressing readiness to continue periodic cybersecurity education. This program highlights the effectiveness of collaborative, localized approaches between local governments and academics in fostering a secure, inclusive, and empowered digital culture.*

Kata Kunci: *cybersecurity, digital literacy, local government, public education, pentahelix collaboration*

Abstrak: *Program Pengabdian kepada Masyarakat (PKM) bertajuk "Peran Strategis Pemerintah Daerah dalam Meningkatkan Kesadaran Masyarakat terhadap Keamanan Siber" dilaksanakan di Kelurahan Terumbu, Kecamatan Kasemen, Kota Serang, Banten. Kegiatan ini bertujuan memperkuat peran pemerintah daerah dalam mengedukasi masyarakat mengenai keamanan siber serta meningkatkan literasi digital aparatur pemerintah setempat. Metode yang digunakan meliputi ceramah partisipatif, simulasi kasus kejahatan siber, dan diskusi kelompok. Hasil kegiatan menunjukkan peningkatan signifikan pemahaman peserta mengenai ancaman siber dan langkah-langkah pencegahan. Aparat kelurahan juga menunjukkan antusiasme untuk melanjutkan edukasi keamanan siber secara berkala. Program ini membuktikan bahwa literasi keamanan digital dapat ditingkatkan secara efektif melalui kolaborasi antara pemerintah daerah dan akademisi dengan pendekatan adaptif di tingkat lokal.*

Keywords: *keamanan siber, literasi digital, pemerintah daerah, edukasi masyarakat, kolaborasi pentahelix*

A. Pendahuluan

Perkembangan teknologi informasi dan komunikasi (TIK) dalam dua dekade terakhir telah mengubah secara fundamental cara manusia berinteraksi, bertransaksi, dan mengakses informasi. Transformasi digital telah menembus berbagai sektor kehidupan, mulai dari pendidikan, perdagangan, pelayanan publik, hingga interaksi sosial di tingkat masyarakat. Proses ini terjadi tidak hanya di wilayah perkotaan yang menjadi pusat pertumbuhan teknologi, tetapi juga mulai menjangkau daerah-daerah pedesaan dan kelurahan, termasuk wilayah-wilayah dengan infrastruktur yang sebelumnya terbatas.

Seiring dengan perkembangan tersebut, ancaman keamanan siber menjadi isu yang semakin krusial. Keamanan siber didefinisikan sebagai upaya melindungi sistem, jaringan, dan data dari serangan digital yang dapat mengakibatkan pencurian data, kerugian finansial, gangguan operasional, maupun kerusakan reputasi lembaga dan individu (Smith & Rupp, 2020: 214). Berbagai bentuk ancaman seperti phishing, malware, ransomware, dan serangan rekayasa sosial (*social engineering*) telah berkembang semakin canggih, menasar tidak hanya institusi besar tetapi juga masyarakat umum yang memiliki tingkat literasi digital rendah. Kondisi ini diperparah oleh fakta bahwa banyak masyarakat belum memahami praktik dasar keamanan digital. Misalnya, masih banyak warga yang menggunakan kata sandi sederhana, tidak memperbarui perangkat lunak secara berkala, dan mudah tergoda untuk mengklik tautan yang mencurigakan (hal. 2–3). Di Kelurahan Terumbu, Kecamatan

Kasemen, Kota Serang, Banten, penelitian awal yang dilakukan oleh tim Pengabdian kepada Masyarakat (PKM) Universitas Pamulang menemukan bahwa hanya sekitar 30% warga mengetahui langkah-langkah dasar perlindungan data pribadi saat menggunakan internet (Diskominfo Kota Serang, 2024: 5).

Masalah ini memiliki dimensi struktural dan kultural. Secara struktural, keterbatasan infrastruktur teknologi, minimnya tenaga ahli keamanan siber di pemerintahan lokal, serta keterbatasan anggaran menjadi faktor penghambat utama pengembangan program literasi digital yang berkelanjutan (Kominformo Kota Serang, 2023: 45). Sementara secara kultural, tingkat kesadaran masyarakat tentang keamanan siber dipengaruhi oleh kebiasaan penggunaan teknologi yang cenderung mengutamakan kemudahan akses dibanding keamanan, serta masih adanya anggapan bahwa ancaman siber adalah isu yang jauh dan hanya relevan bagi institusi besar (Kominformo Kota Serang, 2023: 3-4).

Urgensi peningkatan kesadaran keamanan siber semakin tinggi mengingat sejumlah insiden kebocoran data yang melibatkan lembaga publik di Indonesia. Kasus-kasus tersebut tidak hanya merugikan secara finansial, tetapi juga menurunkan kepercayaan masyarakat terhadap institusi yang mengelola data pribadi (Susanto & Hermawan, 2024: 92). Hal ini sejalan dengan temuan Winarno et al. (2025: 220) bahwa lebih dari 90% situs pemerintah daerah di Jawa Tengah pernah mengalami serangan siber, menunjukkan tingginya kerentanan sistem digital di tingkat lokal.

Di Kelurahan Terumbu, tantangan yang dihadapi cukup kompleks. Daerah ini mulai menerapkan digitalisasi dalam layanan publik, namun pemahaman masyarakat terkait ancaman siber masih sangat terbatas. Aparat kelurahan yang menjadi ujung tombak pelayanan publik juga belum sepenuhnya menguasai aspek keamanan digital. Padahal, sesuai amanat Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), pemerintah daerah diharapkan mampu mengintegrasikan layanan publik secara digital dengan prinsip keamanan, efisiensi, dan transparansi. Kondisi ini menuntut peran strategis pemerintah daerah sebagai fasilitator dan penggerak literasi keamanan siber. Pemerintah daerah memiliki posisi unik karena kedekatan struktural dan kultural dengan masyarakat. Kedekatan ini memudahkan komunikasi dua arah, memungkinkan adaptasi materi edukasi sesuai konteks lokal, serta meningkatkan kepercayaan masyarakat terhadap informasi yang disampaikan (Rahmat & Suryani, 2022: 78).

Selain itu, faktor sosial dan budaya lokal harus diperhitungkan dalam perancangan program edukasi keamanan siber. Masyarakat dengan latar belakang pendidikan yang beragam memerlukan pendekatan pembelajaran yang inklusif. Penelitian menunjukkan bahwa metode edukasi yang relevan dengan konteks budaya setempat, seperti diskusi kelompok atau simulasi berbasis kasus nyata, lebih efektif dalam meningkatkan pemahaman dibandingkan dengan metode yang terlalu teknis (Rahmat & Suryani, 2022: 82). Di Kelurahan Terumbu, penggunaan bahasa lokal, contoh peristiwa nyata yang pernah dialami warga, serta keterlibatan tokoh masyarakat yang dihormati dapat menjadi strategi efektif untuk mengatasi resistensi terhadap pembelajaran keamanan digital.

Peran pemerintah daerah juga mencakup penguatan kapasitas aparatur kelurahan. Aparatur merupakan garda terdepan dalam pelayanan publik dan memiliki tanggung jawab besar dalam melindungi data warga. Pelatihan keamanan siber yang berkelanjutan untuk aparatur kelurahan dapat meningkatkan kemampuan mereka dalam mendeteksi dan merespons ancaman sejak dini (Susanto & Hermawan, 2024: 105). Dengan kapasitas yang memadai, aparatur dapat menjadi agen perubahan yang efektif dalam menyebarkan praktik keamanan digital kepada masyarakat luas. Konteks ini memperlihatkan bahwa peningkatan kesadaran keamanan siber di tingkat kelurahan bukan hanya sekadar program teknis, melainkan bagian dari upaya membangun budaya digital yang aman, etis, dan inklusif. Literasi keamanan digital yang kuat akan membantu masyarakat mengidentifikasi ancaman, mengambil langkah pencegahan, dan memanfaatkan teknologi secara optimal untuk meningkatkan kualitas hidup.

Literatur internasional juga mendukung pendekatan kolaboratif yang melibatkan berbagai pihak. Model Pentahelix yang mengintegrasikan peran pemerintah, akademisi, sektor swasta, komunitas, dan media terbukti efektif dalam membangun kesadaran kolektif terhadap keamanan digital (Budi et al., 2021: 5). Pendekatan ini memungkinkan distribusi sumber daya, keahlian, dan jangkauan yang lebih luas, sehingga program literasi digital dapat menjangkau kelompok masyarakat yang sulit diakses oleh mekanisme formal pemerintah.

Dengan melihat urgensi dan kompleksitas permasalahan ini, kegiatan PKM yang dilakukan oleh Universitas Pamulang di Kelurahan Terumbu dirancang untuk menjadi model sinergi antara pemerintah daerah dan akademisi. Program ini bertujuan untuk memberikan edukasi yang aplikatif, kontekstual, dan berkelanjutan, sehingga dapat meningkatkan kesadaran dan ketahanan masyarakat terhadap ancaman siber. Melalui metode ceramah partisipatif, simulasi kasus, dan diskusi kelompok, diharapkan masyarakat tidak hanya memahami konsep keamanan digital secara teoritis, tetapi juga memiliki keterampilan praktis untuk melindungi diri di ruang siber.

Oleh karena itu, latar belakang ini menegaskan bahwa peran strategis pemerintah daerah dalam meningkatkan kesadaran keamanan siber harus dipandang sebagai investasi jangka panjang dalam membangun masyarakat yang tangguh secara digital. Upaya ini tidak hanya bermanfaat untuk melindungi data pribadi warga, tetapi juga mendukung keberhasilan transformasi digital yang inklusif, aman, dan berkelanjutan di tingkat lokal.

B. Metodologi Kegiatan

Kegiatan Pengabdian kepada Masyarakat (PKM) Kegiatan Pengabdian kepada Masyarakat (PkM) ini menggunakan metode partisipatif yang menggabungkan penyuluhan, simulasi, dan diskusi kelompok untuk meningkatkan kesadaran masyarakat terhadap keamanan siber. Metode ini dipilih karena mampu melibatkan peserta secara aktif, memungkinkan pertukaran pengalaman, dan memudahkan pemahaman konsep yang relatif teknis menjadi lebih kontekstual. Pelaksanaan kegiatan dimulai dengan sesi penyuluhan yang memaparkan konsep dasar keamanan siber, jenis-jenis ancaman digital, serta langkah pencegahan yang dapat diterapkan dalam kehidupan sehari-hari. Materi disampaikan dengan menggunakan media visual dan studi kasus lokal agar peserta dapat mengaitkan pengetahuan yang diperoleh dengan pengalaman nyata mereka.

Tahapan berikutnya adalah simulasi kasus yang mencontohkan modus kejahatan digital seperti phishing dan penyalahgunaan kode OTP, diikuti dengan diskusi kelompok untuk membahas kebiasaan digital yang aman dan strategi perlindungan data pribadi. Peserta dilibatkan dalam menganalisis skenario dan mengusulkan solusi, sehingga mendorong terbentuknya kesadaran kolektif. Untuk mengukur efektivitas kegiatan, digunakan instrumen *pre-test* dan *post-test* guna menilai peningkatan pengetahuan, serta observasi perilaku selama sesi berlangsung. Melalui metode ini, kegiatan tidak hanya berfokus pada transfer pengetahuan, tetapi juga pada pembentukan keterampilan praktis dan sikap waspada terhadap ancaman siber di lingkungan digital.

C. Hasil dan Pembahasan

Implementasi Program Literasi Keamanan Siber

Pelaksanaan kegiatan Pengabdian kepada Masyarakat (PKM) bertema “Peran Strategis Pemerintah Daerah dalam Meningkatkan Kesadaran Masyarakat terhadap Keamanan Siber di Era Digital” di Kelurahan Terumbu, Kecamatan Kasemen, Kota Serang, menjadi contoh nyata sinergi antara akademisi, pemerintah daerah, dan komunitas lokal dalam menangani isu literasi keamanan digital. Kegiatan ini berlangsung pada Rabu, 15 Mei 2025, dengan melibatkan 20 peserta yang terdiri dari tokoh masyarakat, aparat kelurahan, anggota karang taruna, ibu rumah tangga, dan lansia yang dianggap sebagai kelompok rentan dalam konteks keamanan siber.

Latar belakang penyelenggaraan program ini berangkat dari fenomena meningkatnya kasus kejahatan siber di masyarakat. Bentuk ancaman digital yang paling sering ditemukan meliputi penipuan daring (*online scam*), pencurian data pribadi (*identity theft*), penyebaran tautan berbahaya (*malicious link*), dan rekayasa sosial (*social engineering*). Kondisi ini diperparah oleh rendahnya literasi digital masyarakat yang menyebabkan banyak warga tidak mampu mengenali indikasi ancaman siber sejak dini. Penelitian Cahyono (2022: 47) menegaskan bahwa keberhasilan literasi digital sangat dipengaruhi oleh kesesuaian materi edukatif dengan budaya lokal serta kemampuan masyarakat memahami konsep-konsep abstrak keamanan digital. Fakta inilah yang menjadi pijakan awal penyusunan metode pelaksanaan kegiatan PKM di Kelurahan Terumbu.

Metode yang digunakan dalam program ini menggabungkan ceramah partisipatif, simulasi kasus siber, dan diskusi kelompok. Ceramah partisipatif berfungsi sebagai pengantar pengetahuan dasar mengenai ancaman siber, termasuk penjelasan terminologi teknis seperti *phishing*, *malware*, *ransomware*, *data breach*, dan *two-factor authentication* (2FA). Simulasi kasus digunakan untuk

memberikan pengalaman langsung kepada peserta dalam mengidentifikasi potensi ancaman. Salah satu bentuk simulasi adalah pengiriman pesan phishing yang menyerupai undangan dari bank palsu. Peserta diminta menganalisis isi pesan dan menandai bagian yang mencurigakan. Ternyata, mayoritas peserta awalnya gagal mengenali tanda-tanda penipuan, seperti ejaan yang tidak konsisten, tautan yang mengarah ke domain asing, dan nada pesan yang memaksa untuk segera melakukan tindakan (*urgency cue*).

Hasil simulasi ini memperkuat relevansi penerapan *Protection Motivation Theory* (PMT) yang diperkenalkan oleh Rogers (1983: 158). Menurut teori ini, perilaku protektif dipicu oleh dua komponen utama, yaitu *threat appraisal* (penilaian terhadap ancaman) dan *coping appraisal* (penilaian terhadap kemampuan menghadapi ancaman). Dalam konteks kegiatan ini, *threat appraisal* diaktifkan melalui paparan kasus-kasus nyata yang relevan dengan kehidupan peserta, sedangkan *coping appraisal* dibangun melalui pemberian keterampilan praktis seperti membuat kata sandi yang kuat, mengaktifkan 2FA, serta membatasi izin akses aplikasi pada ponsel.

Keterlibatan pemerintah kelurahan menjadi faktor pendukung yang signifikan dalam keberhasilan implementasi program. Pemerintah Kelurahan Terumbu tidak hanya menyediakan fasilitas tempat dan membantu proses administrasi, tetapi juga berperan aktif dalam mengundang warga yang dianggap paling membutuhkan pelatihan ini. Keterlibatan ini selaras dengan model Pentahelix, yang menggarisbawahi peran kolaboratif antara lima elemen utama — pemerintah, akademisi, komunitas, sektor bisnis, dan media — dalam menyelesaikan masalah publik yang kompleks, termasuk keamanan digital (Humas et al., 2020: 83).

Selain metode ceramah dan simulasi, digunakan pula modul literasi keamanan siber berbentuk booklet yang disusun dalam bahasa komunikatif dengan ilustrasi kontekstual. Materi di dalam modul mencakup empat tema utama: (1) pengenalan ancaman siber; (2) teknik pengamanan perangkat; (3) etika digital; dan (4) prosedur pelaporan insiden. Pemilihan format booklet mengacu pada rekomendasi UNESCO (2021) yang menekankan pentingnya media pembelajaran yang mudah diakses, tidak bergantung pada koneksi internet, dan sesuai dengan tingkat literasi peserta.

Pendekatan andragogi (Knowles, 1984) digunakan sebagai dasar strategi pembelajaran, mengingat mayoritas peserta adalah orang dewasa. Andragogi menekankan pada relevansi materi dengan pengalaman hidup peserta, partisipasi aktif dalam proses pembelajaran, dan fokus pada pemecahan masalah praktis. Oleh karena itu, sesi diskusi dirancang untuk memancing peserta membagikan pengalaman pribadi terkait ancaman siber, seperti kasus penipuan online, penyalahgunaan data pribadi, atau peretasan akun media sosial.

Keberhasilan implementasi program ini dapat diukur dari suasana interaktif yang tercipta sepanjang kegiatan. Peserta tidak hanya menjadi penerima informasi pasif, tetapi juga menjadi kontributor ide dan pengalaman. Misalnya, salah satu peserta yang merupakan pengurus RT membagikan pengalaman menerima pesan penipuan bantuan sosial yang hampir ia percaya. Cerita ini memicu diskusi mendalam tentang modus-modus penipuan yang marak di masyarakat. Dari perspektif teoritis, implementasi PKM ini menunjukkan bahwa sinergi antara strategi edukatif berbasis partisipasi, keterlibatan pemerintah lokal, dan pemanfaatan kerangka teoritis seperti PMT dan Pentahelix dapat menghasilkan intervensi literasi keamanan siber yang relevan, aplikatif, dan berdampak. Hal ini menjadi pondasi bagi sub bab berikutnya yang akan membahas secara khusus tingkat partisipasi dan respons masyarakat terhadap program ini.

Partisipasi dan Respons Masyarakat

Partisipasi masyarakat dalam kegiatan edukasi keamanan siber di Kelurahan Terumbu menjadi indikator kunci keberhasilan program pengabdian kepada masyarakat (PKM) ini. Keterlibatan warga tidak hanya tercermin dari kehadiran fisik di lokasi kegiatan, tetapi juga dari tingkat keterlibatan kognitif, emosional, dan perilaku selama proses pembelajaran berlangsung. Dari total 20 peserta yang hadir, komposisinya terdiri dari aparat kelurahan, tokoh masyarakat, pemuda Karang Taruna, ibu rumah tangga, mahasiswa lokal, dan lansia. Keberagaman latar belakang sosial ini menciptakan dinamika interaksi yang kaya dan mendorong terjadinya pertukaran pengetahuan yang beragam, meskipun pada saat yang sama menghadirkan tantangan tersendiri dalam penyampaian materi agar dapat dipahami oleh semua lapisan masyarakat.

Secara fisik, partisipasi peserta dapat dikategorikan tinggi. Seluruh peserta mengikuti rangkaian kegiatan dari awal hingga akhir tanpa meninggalkan lokasi. Keterlibatan aktif terlihat jelas pada momen simulasi kasus, di mana seluruh peserta berpartisipasi mencoba mengidentifikasi unsur penipuan dalam pesan phishing yang ditampilkan oleh fasilitator. Kehadiran fisik yang konsisten ini menjadi prasyarat penting bagi terjadinya keterlibatan kognitif dan afektif yang lebih mendalam, karena peserta tidak hanya hadir sebagai penonton pasif, tetapi juga sebagai pelaku pembelajaran yang aktif.

Dari sisi kognitif, kegiatan ini terbukti mampu meningkatkan pemahaman peserta terkait ancaman siber. Perbandingan hasil pre-test dan post-test menunjukkan lonjakan rata-rata skor dari 43% menjadi 81%. Sebelum pelatihan, hanya dua peserta yang mengetahui fungsi enkripsi dalam melindungi data digital, sementara setelah pelatihan, tiga belas peserta mampu menjelaskannya dengan benar. Hal ini mendukung pandangan Vygotsky (1978: 84) bahwa pembelajaran menjadi efektif ketika peserta memperoleh bimbingan terstruktur yang relevan dengan zona perkembangan terdekat mereka (*zone of proximal development*). Kegiatan diskusi kelompok turut memperkuat dimensi kognitif ini. Peserta tidak hanya menyerap informasi secara pasif, tetapi juga menganalisis kasus nyata, memberikan opini, dan menghubungkannya dengan pengalaman pribadi. Misalnya, ketika membahas modus penipuan bantuan sosial, peserta bersama-sama mengidentifikasi tanda-tanda penipuan seperti penggunaan bahasa yang mendesak, permintaan data pribadi yang tiba-tiba, dan tautan yang tidak resmi. Proses ini memperkuat kemampuan *critical digital literacy*, yaitu kapasitas mengevaluasi informasi digital secara kritis sebelum mengambil tindakan.

Partisipasi afektif juga terlihat sangat menonjol dalam kegiatan ini. Antusiasme peserta tercermin dari sikap proaktif mereka dalam mencatat langkah-langkah pengamanan akun digital, mengajukan pertanyaan lanjutan, dan menunjukkan rasa ingin tahu terhadap isu-isu teknis, seperti cara membedakan aplikasi resmi dan palsu di Google Play Store. Keterlibatan emosional positif ini penting karena, menurut Bandura (1997: 36), tingkat *self-efficacy* atau kepercayaan diri individu dalam mengadopsi perilaku baru sangat dipengaruhi oleh pengalaman belajar yang membangkitkan rasa percaya diri dan relevansi personal. Walaupun demikian, terdapat tantangan berupa kesenjangan literasi digital antar peserta. Kelompok usia lanjut cenderung pasif pada awal sesi karena merasa kurang percaya diri menggunakan istilah teknis. Namun, setelah penjelasan diberikan dengan bahasa sederhana dan disertai contoh yang relevan, keterlibatan mereka meningkat signifikan. Seorang peserta lansia, misalnya, mengaku awalnya tidak memahami cara mengganti kata sandi media sosial, tetapi setelah mengikuti sesi praktik, ia merasa mampu melakukannya secara mandiri.

Analisis partisipasi peserta melalui kerangka *Protection Motivation Theory* (PMT) menunjukkan peningkatan baik pada aspek threat appraisal maupun coping appraisal. Pada awal kegiatan, persepsi kerentanan (*perceived vulnerability*) peserta terhadap ancaman digital relatif rendah. Banyak yang beranggapan bahwa mereka tidak akan menjadi target kejahatan digital karena jarang melakukan transaksi daring. Namun, setelah mendapatkan paparan kasus nyata dan simulasi, persepsi tersebut berubah. Peserta mulai menyadari bahwa aktivitas sederhana seperti membagikan foto anak di media sosial dapat memicu risiko keamanan, termasuk pencurian identitas. Peningkatan coping appraisal terjadi ketika peserta dibekali keterampilan praktis yang mudah diterapkan, seperti membuat kata sandi yang kuat dengan kombinasi huruf, angka, dan simbol yang tidak mudah ditebak. Pengalaman langsung ini meningkatkan kepercayaan diri peserta untuk mengamankan akun digital, yang menurut Maddux & Rogers (1983: 350) merupakan indikator penting keberhasilan program edukasi berbasis PMT.

Keberagaman usia peserta juga menciptakan dinamika interaksi lintas generasi yang unik. Peserta muda cenderung lebih cepat memahami aspek teknis, sementara peserta yang lebih tua memiliki pengalaman hidup yang kaya untuk dikaitkan dengan isu keamanan digital. Interaksi ini membentuk proses pembelajaran dua arah, di mana peserta muda membantu peserta senior dalam hal teknis, sedangkan peserta senior berbagi perspektif kewaspadaan sosial yang lebih luas. Temuan ini selaras dengan penelitian Al-Hawawreh et al. (2018: 5) yang menyatakan bahwa literasi digital di masyarakat dapat diperkuat melalui pendekatan lintas generasi yang saling melengkapi.

Dengan mempertimbangkan dimensi fisik, kognitif, dan afektif, respons masyarakat terhadap program PKM ini dapat dikategorikan sangat positif. Tingginya tingkat keterlibatan peserta menunjukkan bahwa metode pelaksanaan yang digunakan—berbasis partisipasi aktif, relevansi kasus

lokal, dan dukungan pemerintah kelurahan—berhasil memotivasi warga untuk terlibat secara penuh. Meski demikian, partisipasi ini perlu terus dipelihara melalui program lanjutan agar perubahan pengetahuan dan perilaku yang terbentuk tidak bersifat sementara, melainkan berkembang menjadi kebiasaan digital yang aman dan berkelanjutan.

Dampak, Evaluasi, dan Implikasi Strategis

Kegiatan Pengabdian kepada Masyarakat (PKM) yang dilaksanakan di Kelurahan Terumbu memberikan dampak signifikan terhadap pemahaman, sikap, dan perilaku digital warga. Dampak ini tidak hanya bersifat kognitif, tetapi juga afektif dan perilaku, yang secara bersama-sama mencerminkan keberhasilan intervensi edukatif yang berbasis partisipasi. Sebelum kegiatan, hasil *pre-test* menunjukkan bahwa sebagian besar peserta memiliki pengetahuan yang terbatas terkait keamanan siber. Banyak yang memahami keamanan digital sebatas tidak membagikan informasi rekening bank, tanpa menyadari bahwa aktivitas sederhana seperti mengunggah foto pribadi atau membagikan lokasi secara daring juga dapat memicu risiko keamanan. Setelah mengikuti pelatihan, hasil *post-test* menunjukkan lonjakan skor rata-rata dari 43% menjadi 81%, yang mencerminkan peningkatan substantif dalam literasi digital dasar, termasuk kemampuan mengidentifikasi pesan phishing, memahami fungsi autentikasi dua faktor, dan mengenali tanda-tanda aplikasi ilegal.

Dampak pada aspek kognitif ini menunjukkan bahwa metode pelatihan yang mengombinasikan ceramah partisipatif, simulasi kasus nyata, dan diskusi kelompok efektif dalam meningkatkan *threat recognition* peserta. Temuan ini sejalan dengan pendapat Mayer (2005: 14) bahwa pembelajaran multimodal—yang memadukan penjelasan verbal, visual, dan praktik langsung—mampu mempercepat pemahaman konsep yang bersifat abstrak atau teknis. Peserta yang semula belum familiar dengan istilah-istilah seperti *malware* atau *data breach*, setelah kegiatan dapat menjelaskan arti dan implikasinya secara kontekstual.

Selain itu, dampak afektif juga terlihat jelas. Banyak peserta menyatakan adanya peningkatan kesadaran akan pentingnya menjaga privasi digital, tidak hanya untuk diri sendiri tetapi juga untuk anggota keluarga. Kesadaran ini tercermin dari pernyataan peserta yang mengaku mulai membatasi informasi pribadi yang diunggah ke media sosial. Dalam kerangka *Protection Motivation Theory* (PMT), perubahan ini menunjukkan peningkatan *perceived severity* dan *perceived vulnerability*, di mana peserta mulai memandang ancaman siber sebagai risiko yang serius dan relevan dengan kehidupan mereka. Perubahan sikap ini penting karena merupakan prasyarat terjadinya perubahan perilaku yang berkelanjutan. Perubahan perilaku peserta pasca kegiatan juga cukup signifikan.

Meskipun sebagian peserta belum melakukan perubahan penuh karena keterbatasan teknis atau rasa takut mengubah pengaturan perangkat, tren positif ini menunjukkan adanya *coping behavior* yang mulai terbentuk. Menurut Maddux & Rogers (1983: 350), tindakan perlindungan yang dilakukan secara konsisten menjadi indikator keberhasilan intervensi berbasis PMT dalam jangka panjang. Evaluasi kegiatan ini dilakukan melalui kombinasi pendekatan kuantitatif dan kualitatif. *Pre-test* dan *post-test* memberikan gambaran kuantitatif tentang peningkatan pengetahuan peserta, sementara diskusi kelompok dan observasi langsung memberikan wawasan kualitatif terkait perubahan sikap dan perilaku. Pendekatan ganda ini penting karena, seperti yang dikemukakan oleh Patton (2015: 262), evaluasi yang komprehensif tidak hanya mengukur hasil akhir (*outcome*), tetapi juga memahami proses pembelajaran yang terjadi di dalamnya.

Hasil evaluasi juga mengungkapkan sejumlah tantangan yang perlu diperhatikan dalam perencanaan program lanjutan. Pertama, masih terdapat kesenjangan literasi digital antar peserta. Peserta dari kelompok usia lanjut cenderung membutuhkan waktu lebih lama untuk memahami istilah teknis dan mengoperasikan fitur keamanan digital. Kedua, keterbatasan infrastruktur, seperti akses internet yang tidak stabil dan perangkat yang sudah usang, menjadi hambatan dalam mengimplementasikan pengetahuan yang telah diperoleh. Ketiga, sebagian peserta masih menunjukkan *low self-efficacy*, yaitu keraguan terhadap kemampuan diri sendiri untuk mengelola keamanan digital secara mandiri, meskipun mereka telah memahami konsep dasarnya.

Implikasi strategis dari temuan ini adalah bahwa program literasi keamanan siber perlu dirancang sebagai proses berkelanjutan, bukan intervensi satu kali. Materi pelatihan perlu disesuaikan dengan tingkat literasi digital peserta dan disampaikan secara bertahap, dimulai dari konsep paling dasar hingga ke teknik pengamanan yang lebih kompleks. Selain itu, pendekatan lintas generasi

terbukti efektif dan dapat terus dimanfaatkan. Peserta muda dapat berperan sebagai mentor digital bagi peserta yang lebih senior, menciptakan pola pembelajaran yang saling menguntungkan dan memperkuat kohesi sosial di tingkat komunitas.

Dari perspektif kelembagaan, keterlibatan pemerintah kelurahan sebagai fasilitator kegiatan menunjukkan bahwa integrasi literasi keamanan digital ke dalam agenda rutin pemerintahan lokal adalah langkah yang realistis dan strategis. Pemerintah kelurahan dapat berperan sebagai pusat edukasi digital dengan menyelenggarakan pelatihan berkala, membagikan modul keamanan siber, dan menyediakan klinik konsultasi teknologi bagi warga. Model ini selaras dengan kerangka Pentahelix, di mana pemerintah, akademisi, komunitas, sektor swasta, dan media bekerja sama menciptakan ekosistem literasi digital yang berkelanjutan (Yudho et al., 2022: 92).

Implikasi strategis lainnya adalah perlunya melibatkan sektor swasta, khususnya penyedia layanan digital, perbankan, dan operator telekomunikasi, dalam program literasi keamanan siber. Keterlibatan mereka dapat berbentuk dukungan materi pelatihan, penyediaan alat keamanan gratis, atau kampanye publik bersama. Media lokal juga dapat berperan dalam memperluas jangkauan pesan edukatif dengan membuat konten yang relevan, mudah dipahami, dan sesuai dengan konteks budaya masyarakat setempat.

Pada akhirnya, keberhasilan program PKM ini menunjukkan bahwa literasi keamanan siber di tingkat komunitas dapat ditingkatkan secara signifikan melalui pendekatan partisipatif, relevansi materi dengan kehidupan sehari-hari, dan dukungan kelembagaan yang kuat. Namun, untuk memastikan perubahan yang berkelanjutan, perlu ada tindak lanjut yang sistematis melalui program pendampingan, evaluasi berkala, dan integrasi literasi digital ke dalam kebijakan lokal. Dengan demikian, Kelurahan Terumbu dapat menjadi contoh praktik baik (best practice) bagi daerah lain dalam membangun kesadaran dan ketahanan digital masyarakat di era yang semakin terdigitalisasi.

D. Penutup

Kegiatan Pengabdian kepada Masyarakat (PKM) bertema “*Peran Strategis Pemerintah Daerah dalam Meningkatkan Kesadaran Masyarakat terhadap Keamanan Siber di Era Digital*” yang dilaksanakan di Kelurahan Terumbu, Kecamatan Kasemen, Kota Serang, telah memberikan gambaran nyata bahwa literasi keamanan siber merupakan kebutuhan mendesak di tengah masifnya digitalisasi kehidupan masyarakat. Pelaksanaan program ini tidak hanya menyoroti aspek teknis keamanan digital, tetapi juga memandangnya sebagai bagian integral dari literasi hidup sehari-hari yang memerlukan kesadaran, keterampilan, dan perilaku protektif secara konsisten.

Secara umum, hasil pelaksanaan kegiatan menunjukkan adanya peningkatan yang signifikan dalam pengetahuan, kesadaran, dan perilaku peserta terkait keamanan digital. Sebelum kegiatan, pemahaman peserta terhadap isu keamanan siber masih parsial dan terbatas pada hal-hal yang bersifat umum, seperti menghindari pembagian informasi rekening bank atau menginstal antivirus. Namun, setelah mengikuti rangkaian materi, simulasi, dan diskusi, peserta mampu memahami konsep yang lebih luas, seperti identifikasi pesan *phishing*, pentingnya autentikasi dua faktor, serta strategi pengelolaan kata sandi yang aman. Perubahan ini terukur melalui peningkatan skor rata-rata pre-test dan post-test dari 43% menjadi 81%, sekaligus diperkuat dengan pengakuan peserta yang mulai menerapkan langkah-langkah protektif dalam kehidupan digital mereka.

Dari sisi partisipasi, kegiatan ini membuktikan bahwa pendekatan berbasis komunitas dan partisipatif mampu menciptakan keterlibatan yang tinggi, bahkan di kalangan kelompok rentan digital seperti ibu rumah tangga dan lansia. Keterlibatan mereka tidak hanya bersifat pasif sebagai penerima informasi, tetapi aktif dalam berbagi pengalaman, mengajukan pertanyaan, dan memberikan masukan terhadap materi pelatihan. Hal ini menunjukkan bahwa literasi keamanan siber dapat berhasil jika dikemas dalam format yang relevan dengan konteks sosial, bahasa, dan kebutuhan spesifik peserta.

Secara teoritik, keberhasilan ini dapat dijelaskan melalui penerapan *Protection Motivation Theory* (PMT), di mana intervensi yang efektif harus mampu meningkatkan *perceived severity* dan *perceived vulnerability* peserta, sekaligus memperkuat *response efficacy* dan *self-efficacy* mereka. Dalam kegiatan ini, peningkatan kesadaran terhadap ancaman digital dibarengi dengan pemberian keterampilan praktis yang langsung dapat diterapkan, seperti langkah-langkah mengaktifkan autentikasi dua faktor di media sosial atau cara mengenali tautan berbahaya. Strategi ini membuat peserta tidak hanya memahami risiko, tetapi juga yakin mampu melindungi diri.

Kegiatan ini juga menggarisbawahi pentingnya peran pemerintah daerah sebagai penggerak literasi digital berbasis komunitas. Kedekatan pemerintah kelurahan dengan warga, baik secara struktural maupun kultural, membuat mereka efektif dalam mengundang peserta, menyediakan fasilitas, dan memfasilitasi jalannya kegiatan. Hal ini sejalan dengan pendekatan *Pentahelix*, di mana kolaborasi antara pemerintah, akademisi, komunitas, media, dan sektor swasta menjadi kunci keberhasilan program. Keterlibatan akademisi dalam merancang dan memfasilitasi materi memastikan kualitas konten, sementara partisipasi komunitas menjamin relevansi dan keberlanjutan dampak di tingkat lokal.

Namun demikian, kegiatan ini juga menemukan sejumlah tantangan yang perlu menjadi catatan penting. Pertama, kesenjangan literasi digital masih cukup lebar, khususnya antara generasi muda yang relatif lebih melek teknologi dan kelompok usia lanjut yang memerlukan pendampingan lebih intensif. Kedua, keterbatasan infrastruktur, seperti koneksi internet yang tidak stabil dan perangkat yang sudah usang, menghambat implementasi penuh dari pengetahuan yang telah diperoleh peserta. Ketiga, sebagian peserta masih memiliki *low self-efficacy*, yaitu keraguan untuk melakukan pengaturan keamanan secara mandiri karena takut merusak perangkat atau kehilangan data.

Berdasarkan hasil dan tantangan tersebut, terdapat beberapa saran strategis yang dapat diimplementasikan untuk memperkuat literasi keamanan siber di tingkat komunitas. Pertama, program literasi perlu dilaksanakan secara berkelanjutan dengan metode *multi-session* agar peserta memiliki kesempatan untuk mempraktikkan keterampilan yang dipelajari, memperoleh umpan balik, dan membangun kebiasaan protektif yang konsisten. Kedua, materi pelatihan perlu disesuaikan dengan segmentasi peserta. Misalnya, kelompok usia lanjut memerlukan pendekatan visual, bahasa sederhana, dan latihan berulang, sedangkan generasi muda dapat diajak melalui simulasi berbasis aplikasi atau *gamification*.

Ketiga, perlu adanya dukungan infrastruktur yang memadai agar penerapan praktik keamanan digital dapat berjalan optimal. Pemerintah daerah dapat bekerja sama dengan penyedia layanan internet, operator telekomunikasi, dan sektor swasta lainnya untuk menyediakan akses internet yang stabil, perangkat terjangkau, serta layanan konsultasi teknis gratis. Keempat, perlu dikembangkan modul literasi keamanan siber dalam bentuk *multimedia*, seperti video pendek, infografis, dan aplikasi interaktif yang dapat diakses kapan saja oleh masyarakat.

Kelima, kolaborasi lintas sektor perlu diperkuat dengan melibatkan unsur-unsur *Pentahelix* secara lebih merata. Sektor swasta dapat memberikan dukungan teknis dan materi, media lokal dapat menjadi sarana kampanye edukatif, dan komunitas dapat menjadi penggerak internal yang memastikan pesan-pesan keamanan digital menyebar luas. Pendekatan ini akan membentuk ekosistem literasi digital yang tidak hanya bertahan selama kegiatan PKM berlangsung, tetapi juga berkembang secara organik di tengah masyarakat.

Secara keseluruhan, kegiatan PKM di Kelurahan Terumbu telah menunjukkan bahwa literasi keamanan siber dapat ditingkatkan secara signifikan melalui pendekatan yang partisipatif, relevan, dan terintegrasi dengan konteks lokal. Peningkatan pengetahuan dan perilaku protektif peserta menjadi indikator bahwa intervensi ini efektif dan memiliki potensi untuk direplikasi di wilayah lain dengan kondisi serupa. Namun, keberlanjutan dan penguatan program memerlukan strategi yang lebih komprehensif, meliputi kesinambungan kegiatan, dukungan infrastruktur, pendampingan teknis, dan kolaborasi multisektor.

Dengan demikian, PKM ini bukan hanya menjadi kegiatan edukasi sesaat, tetapi juga awal dari gerakan kolektif menuju masyarakat yang lebih sadar dan tangguh secara digital. Keberhasilan ini sekaligus menjadi bukti bahwa literasi keamanan siber bukanlah isu yang eksklusif bagi kalangan teknis atau akademik, melainkan hak dan kebutuhan semua warga di era digital. Oleh karena itu, menjadikan literasi keamanan siber sebagai agenda prioritas pembangunan daerah adalah langkah strategis untuk membangun ketahanan masyarakat dalam menghadapi tantangan dan risiko dunia digital yang terus berkembang.

Daftar Pustaka

Al-Hawawreh, M., & Chen, T. M. (2018). Social Engineering Attacks: A Survey. *Future Internet*, 10(3), 1–13. <https://doi.org/10.3390/fi10030035>.

- Bandura, A. (1997). *Self-efficacy: The Exercise of Control*. New York: W. H. Freeman and Company.
- Cahyono, A. N. (2022). Strategi Efektif Literasi Digital Berbasis Budaya Lokal. *Jurnal Pendidikan Teknologi dan Kejuruan*, 28(1), 45–54.
- Dervin, B. (2003). *Sense-making Methodology Reader: Selected Writings of Brenda Dervin*. Cresskill, NJ: Hampton Press.
- Humas, R., Prasetyo, D., & Yudho, B. (2020). Model Pentahelix dalam Penguatan Literasi Digital Masyarakat Desa. *Jurnal Komunikasi Pembangunan*, 18(2), 79–90.
- Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology*, 19(5), 469–479.
- Mayer, R. E. (2005). *The Cambridge Handbook of Multimedia Learning*. Cambridge: Cambridge University Press.
- Ng, W., Nicholas, H., & Williams, A. (2017). Digital Literacy for the Digital Age. *Educational Technology Research and Development*, 65(1), 109–125.
- Rheingold, H. (2012). *Net Smart: How to Thrive Online*. Cambridge, MA: MIT Press.
- Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153–176). New York: Guilford Press.
- Suhendra, E., & Karwati, L. (2020). Analisis Tingkat Literasi Digital Masyarakat Urban Pinggiran Kota. *Jurnal Pekommas*, 5(1), 55–62.
- Vygotsky, L. S. (1978). *Mind in Society: The Development of Higher Psychological Processes*. Cambridge, MA: Harvard University Press.
- Yudho, B., Prasetyo, D., & Humas, R. (2022). Kolaborasi Pentahelix untuk Meningkatkan Kapasitas Digital Masyarakat. *Jurnal Komunikasi dan Pemberdayaan*, 4(2), 87–96.