

Edukasi Keamanan Siber Berdigital dengan Aman

Feliks Prasepta Sejahtera Surbakti*

Universitas Katolik Indonesia Atma Jaya, Jakarta, Indonesia

*Corresponding Author: feliks.prasepta@atmajaya.ac.id

Info Artikel Diterima: 16/11/2024 Direvisi: 26/11/2024 Disetujui: 28/11/2024

Abstract. *The rapid development of digital technology in Indonesia has heightened the need for cybersecurity education to safeguard individuals against prevalent digital fraud. This community service initiative, titled "Cybersecurity: Safe Digital Practices," aims to raise awareness and educate participants about key aspects of digital security. The program covers the fundamentals of cybersecurity, including digital fraud detection, device security, identity protection, and understanding digital footprints. The implementation involved interactive workshops that addressed common cyber threats and equipped participants with practical strategies for safe digital engagement. Methodologies included presentations on real-life cyber-attack cases, discussions on digital fraud tactics such as phishing, pharming, and sniffing, and hands-on sessions for using security tools like two-factor authentication, fingerprint authentication, and device tracking. Participants were encouraged to engage actively, allowing for the immediate application of learned strategies. Results indicate an increased awareness and capability among participants to recognize and counteract digital fraud. Through post-program evaluations, participants reported a significant improvement in their confidence and ability to protect personal information and secure digital devices. In conclusion, this program effectively enhanced the cybersecurity skills of the participants. It is recommended that future programs expand to include more advanced topics, such as cybersecurity for small businesses and data privacy laws. Continued collaboration with educational institutions and community organizations can further disseminate cybersecurity knowledge across broader demographics, ensuring safer digital practices at the community level.*

Keywords: *Cybersecurity, Digital fraud, Identity and device protection.*

Abstrak. Perkembangan pesat teknologi digital di Indonesia meningkatkan kebutuhan akan edukasi keamanan siber untuk melindungi individu dari penipuan digital yang semakin marak terjadi. Program pengabdian masyarakat ini, yang berjudul "Keamanan Siber: Berdigital dengan Aman," bertujuan untuk meningkatkan kesadaran dan edukasi masyarakat tentang aspek-aspek utama keamanan digital. Program ini mencakup dasar-dasar keamanan siber, termasuk deteksi penipuan digital, keamanan perangkat, perlindungan identitas, dan pemahaman rekam jejak digital. Pelaksanaan kegiatan pengabdian masyarakat ini melibatkan webinar interaktif yang membahas ancaman siber umum dan membekali peserta dengan strategi praktis untuk terlibat secara digital dengan aman. Metodologi yang digunakan meliputi presentasi kasus nyata serangan siber, diskusi tentang taktik penipuan digital seperti phishing, pharming, dan sniffing, serta sesi praktik langsung dalam penggunaan alat keamanan seperti otentikasi dua faktor, otentikasi sidik jari, dan pelacakan perangkat. Peserta didorong untuk terlibat secara aktif sehingga dapat langsung menerapkan strategi yang dipelajari. Hasil menunjukkan peningkatan kesadaran dan kemampuan peserta dalam mengenali dan melawan penipuan digital. Melalui evaluasi pasca-kegiatan pengabdian masyarakat, peserta webinar menunjukkan peningkatan signifikan dalam kepercayaan diri dan kemampuan mereka untuk melindungi informasi pribadi serta mengamankan perangkat digital. Kesimpulannya, kegiatan pengabdian masyarakat ini secara efektif meningkatkan keterampilan keamanan siber bagi para peserta. Untuk lanjutan kegiatan pengabdian masyarakat, direkomendasikan agar materi mencakup topik yang lebih lanjut, seperti keamanan siber untuk usaha kecil dan pembahasan undang-undang privasi data. Kolaborasi berkelanjutan dengan institusi pendidikan dan organisasi masyarakat dapat semakin menyebarkan pengetahuan keamanan siber pada demografi yang lebih luas, memastikan praktik digital yang aman di segala lapisan masyarakat.

Kata Kunci:Keamanan siber, Penipuan digital, Perlindungan identitas dan perangkat.

How to Cite: Surbakti, F. P. S. (2024). Edukasi Keamanan Siber Berdigital dengan Aman. *Prima Abdika: Jurnal Pengabdian Masyarakat*, 4(4), 868-878. <https://doi.org/10.37478/abdika.v4i4.4967>



Copyright (c) 2024 Feliks Prasepta Sejahtera Surbakti. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Pendahuluan

Dalam era digital saat ini, keamanan siber menjadi aspek penting yang harus diperhatikan oleh setiap individu maupun Lembaga (Abdullah & Iksari, 2023). Tingginya tingkat adopsi teknologi digital di Indonesia, termasuk dalam penggunaan media sosial, aplikasi perbankan, dan transaksi *online*, membawa dampak positif berupa kemudahan akses dan efisiensi. Namun, di sisi lain, hal ini juga meningkatkan risiko terjadinya kejahatan siber. Laporan terbaru menunjukkan peningkatan jumlah serangan siber yang signifikan, baik dalam bentuk pencurian data maupun penipuan digital. Serangan terhadap data pribadi dan institusi menjadi masalah serius, seperti yang terlihat dari beberapa insiden besar di Indonesia, termasuk peretasan

data BPJS Kesehatan, BRI Life, dan beberapa lembaga pemerintah lainnya yang telah merugikan berbagai pihak (Firdaus, 2022).

Tantangan dalam menghadapi masalah keamanan siber ini adalah kurangnya kesadaran dan pemahaman masyarakat akan pentingnya praktik-praktik keamanan digital (Islami, 2018). Banyak masyarakat belum sepenuhnya memahami risiko yang timbul dari tindakan sederhana seperti penggunaan kata sandi yang lemah, kurangnya pengamanan pada perangkat digital, serta minimnya pengetahuan tentang penipuan digital seperti *phishing* dan *pharming* (Marwati & Astofa, 2024). Padahal, serangan semacam ini seringkali memanfaatkan kelengahan pengguna yang kurang memahami konsep dasar keamanan siber.

Kebutuhan akan edukasi keamanan siber menjadi sangat mendesak, terutama untuk meningkatkan kesadaran akan pentingnya melindungi data pribadi di tengah maraknya kejahatan siber (Kasim et al., 2022). Edukasi ini tidak hanya bertujuan melindungi masyarakat dari ancaman yang berpotensi merugikan secara finansial, tetapi juga dari dampak psikologis yang sering kali timbul akibat pelanggaran privasi dan pencurian identitas. Dengan memberikan pengetahuan dasar mengenai langkah-langkah perlindungan data, diharapkan masyarakat dapat lebih bijak dalam beraktivitas secara digital (Sari, 2023).

Program pengabdian masyarakat ini, yang bertajuk "Keamanan Siber: Berdigital dengan Aman," disusun untuk mengatasi masalah tersebut dengan memberikan pemahaman yang lebih mendalam mengenai keamanan digital. Program ini mencakup beberapa topik utama seperti deteksi penipuan digital, pengamanan perangkat, perlindungan identitas digital, dan pemahaman akan rekam jejak digital. Melalui pendekatan yang interaktif dan aplikatif, peserta didorong untuk memahami berbagai bentuk ancaman siber serta cara-cara efektif untuk menghadapinya dalam kehidupan sehari-hari.

Studi pustaka menunjukkan bahwa program edukasi keamanan siber telah terbukti efektif dalam mengurangi risiko kejahatan digital, terutama bagi kelompok masyarakat yang rentan. Kajian yang dilakukan oleh (Algamar & Ampri, 2022; Herawati et al., 2024; Krisnaningsih et al., 2023; Sidiq, 2024) menekankan pentingnya pemahaman tentang rekam jejak digital dan langkah-langkah pengamanan, yang sangat relevan dalam konteks penggunaan teknologi informasi di masyarakat Indonesia. Referensi ini menunjukkan bahwa edukasi tentang praktik keamanan digital memiliki dampak signifikan dalam meningkatkan kesadaran dan kemampuan masyarakat dalam menghadapi risiko siber.

Masalah keamanan siber telah menjadi perhatian banyak peneliti karena meningkatnya risiko kejahatan digital di berbagai kalangan masyarakat. Beberapa penelitian sebelumnya menjadi acuan dalam penyusunan dan pelaksanaan program pengabdian masyarakat ini. Algamar and Ampri (2022) menyoroti pentingnya penghapusan jejak digital untuk melindungi privasi individu, khususnya dari ancaman *deepfake* (Gandrova & Banke, 2023). Penelitian ini memberikan wawasan mengenai kebutuhan akan literasi keamanan digital, terutama dalam mengenali risiko yang muncul dari rekam jejak digital yang tidak terlindungi. Sidiq (2024) menyebutkan pentingnya literasi digital untuk menciptakan media sosial yang aman dan nyaman. Penelitian ini memberikan kerangka kerja bagi program ini dalam mengajarkan penggunaan teknologi yang bijak.

Tema keamanan siber telah menjadi subjek berbagai kegiatan pengabdian masyarakat sebelumnya, yang bertujuan meningkatkan literasi

digital masyarakat. Pada PKM "*Digital Safety Awareness* untuk Pelajar SMA" oleh Herawati et al. (2024), program ini berfokus pada siswa SMA, dengan pendekatan edukasi berbasis modul dan diskusi kelompok kecil untuk mengenalkan dasar-dasar keamanan digital, termasuk perlindungan privasi di media sosial. Sementara pengabdian masyarakat yang dilakukan menargetkan masyarakat umum dengan latar belakang dan kebutuhan keamanan digital yang lebih beragam. Selain itu, metode yang digunakan pada kegiatan pengabdian ini lebih interaktif dengan simulasi langsung menggunakan alat keamanan digital seperti autentikasi dua faktor. Yang kedua yang dibandingkan adalah PKM "*Membangun Keamanan Siber untuk UMKM*" oleh Daeng et al. (2023). Program ini ditujukan kepada pelaku usaha kecil dan menengah (UMKM) untuk melindungi data bisnis mereka dari ancaman siber. Pendekatannya mencakup pelatihan tentang keamanan transaksi digital dan pengelolaan data pelanggan. Sementara itu, pengabdian masyarakat yang dilakukan pada kegiatan ini menargetkan individu, bukan sektor bisnis. Perbedaan lain adalah pendekatan program lebih berfokus pada perlindungan data pribadi dan perangkat yang digunakan dalam kehidupan sehari-hari, bukan data bisnis.

Tujuan dari kegiatan pengabdian masyarakat ini adalah memberikan edukasi kepada masyarakat mengenai langkah-langkah praktis dan mudah diterapkan dalam menjaga keamanan data pribadi dan perangkat digital mereka. Program ini diharapkan mampu meningkatkan literasi keamanan digital di kalangan masyarakat, sehingga mereka tidak hanya menjadi pengguna teknologi yang bijak tetapi juga mampu melindungi diri dari berbagai bentuk kejahatan siber yang terus berkembang.

Metode Pelaksanaan

Program pengabdian masyarakat "*Keamanan Siber: Berdigital dengan Aman*" ini dilaksanakan melalui beberapa tahapan untuk memastikan efektivitas dalam meningkatkan literasi keamanan digital masyarakat. Tahapan pertama adalah persiapan dan perencanaan kegiatan, yang meliputi analisis kebutuhan dan identifikasi target peserta. Berdasarkan identifikasi awal, peserta yang paling membutuhkan edukasi ini adalah masyarakat umum, khususnya pengguna aktif internet yang belum memiliki pengetahuan dasar tentang keamanan siber. Materi disusun mencakup berbagai aspek penting seperti dasar-dasar keamanan siber (Daeng et al., 2023), pengenalan jenis-jenis serangan digital (Saputra et al., 2023), dan cara-cara melindungi data pribadi serta perangkat (Yel & Nasution, 2022).

Tahap kedua adalah penyusunan materi dan perancangan alat evaluasi. Materi kegiatan meliputi topik-topik esensial seperti mengenali dan menghindari penipuan digital (*phishing*, *pharming*, dan *sniffing*), pengamanan perangkat digital melalui penggunaan kata sandi yang kuat, serta pentingnya autentikasi dua faktor (Hasya et al., 2024). Selain itu, disiapkan juga alat bantu visual berupa infografis dan video pendek untuk memperjelas penyampaian konsep kepada peserta. Alat evaluasi berupa *pre-test* dan *post-test* disiapkan untuk mengukur tingkat pemahaman peserta sebelum dan sesudah kegiatan pengabdian masyarakat berlangsung.

Tahap ketiga adalah pelaksanaan kegiatan edukasi, yang dibagi menjadi beberapa sesi interaktif. Pada sesi pertama, peserta diperkenalkan dengan berbagai jenis ancaman digital melalui studi kasus yang relevan, seperti kasus peretasan data BPJS dan BRI Life (Nasrudin & Latumahina, 2022; Rahma et al., 2023). Peserta diajak berdiskusi dan menggali dampak

dari kejahatan siber tersebut, serta memahami bagaimana ancaman ini dapat terjadi dalam kehidupan sehari-hari. Kegiatan ini bertujuan untuk meningkatkan kesadaran peserta akan risiko yang mereka hadapi saat beraktivitas secara digital.

Pada sesi berikutnya, peserta diberikan pemahaman tentang praktik keamanan perangkat dan identitas digital. Dalam sesi ini, disampaikan langkah-langkah sederhana namun efektif, seperti penggunaan aplikasi keamanan, otentikasi sidik jari, dan fitur pelacakan perangkat yang tersedia di *smartphone* (Saputri, 2023). Sesi ini juga melibatkan latihan langsung di mana peserta diminta untuk mengatur kata sandi yang kuat, mengaktifkan otentikasi dua faktor, serta memahami fungsi "*Find My Device*" untuk menjaga keamanan perangkat (Putri et al., 2023; Tarigan et al., 2024). Selanjutnya, dilakukan evaluasi kegiatan melalui *post-test* untuk mengukur efektivitas penyampaian materi. Evaluasi ini bertujuan untuk mengetahui peningkatan pemahaman peserta setelah mengikuti program. Berdasarkan hasil evaluasi, dapat dilihat seberapa besar perubahan dalam kemampuan peserta untuk mengenali dan melindungi diri dari ancaman digital.

Tahap akhir adalah penyusunan laporan dan rekomendasi. Laporan ini mencakup hasil dari seluruh rangkaian kegiatan, tingkat pemahaman peserta sebelum dan sesudah kegiatan, serta tantangan yang dihadapi selama pelaksanaan. Rekomendasi yang diberikan antara lain adalah perlunya mengadakan kegiatan lanjutan dengan topik yang lebih mendalam, seperti privasi data dan undang-undang keamanan digital. Dengan metode pelaksanaan yang komprehensif ini, diharapkan masyarakat semakin siap menghadapi tantangan keamanan siber dalam kehidupan digital mereka sehari-hari.

Webinar Nasional dengan tema "Keamanan Siber: Berdigital dengan Aman" diselenggarakan oleh Kementerian Komunikasi dan Informatika (Kemkominfo) bekerja sama dengan Komisi I Dewan Perwakilan Rakyat Republik Indonesia (DPR RI). Seluruh acara webinar difasilitasi oleh Studio Intel Pasar Minggu, yang ditunjuk oleh Kemkominfo, berlokasi di Jalan Tik. Peleng No.B/32, RT.4/RW.8, Pasar Minggu, Jakarta Selatan, Daerah Khusus Ibukota Jakarta, 12520. Universitas Katolik Indonesia Atma Jaya sebelumnya telah berkolaborasi dengan Studio Intel Pasar Minggu dalam penyelenggaraan webinar nasional lainnya berjudul "Membangun Masa Depan Cerah bagi Generasi Z," yang menargetkan siswa sekolah menengah atas yang terdaftar dalam Program Studi Teknik Industri (Prasetya & Surbakti, 2023; Surbakti, 2024).



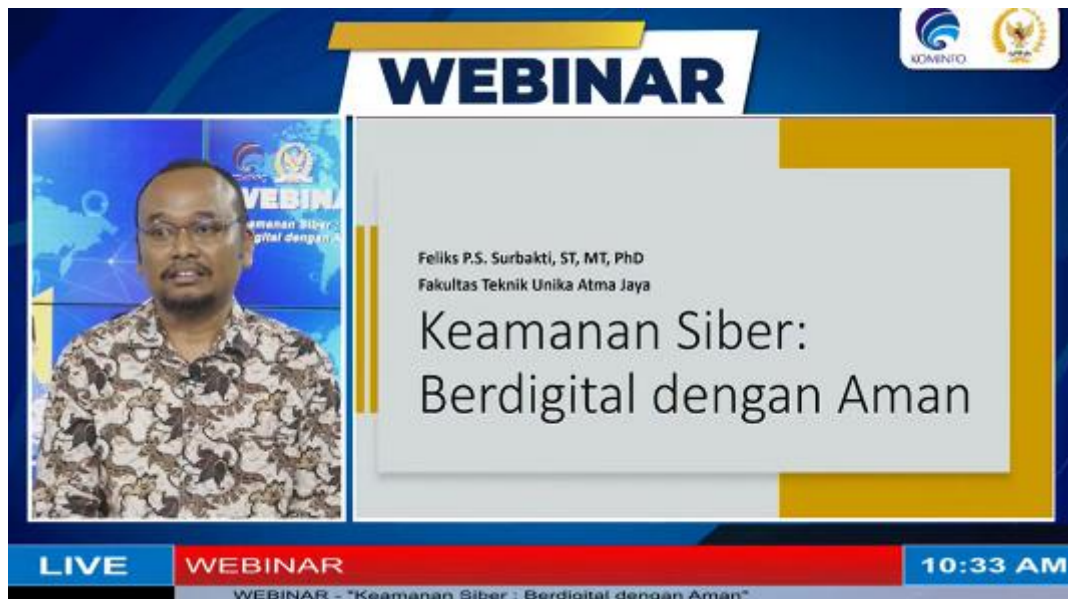
Gambar 1. Flyer acara dan materi presentasi webinar yang disusun

Selama fase persiapan, para pembicara mempersiapkan, menyusun, dan menyampaikan materi berdasarkan topik yang telah ditentukan. Acara ini menghadirkan tiga pembicara: Kresna Dewanata Phrosakh (anggota Komisi I Dewan Perwakilan Rakyat Republik Indonesia), Feliks Prasepta Sejahtera Surbakti, S.T., M.T., PhD (dosen Universitas Katolik Indonesia Atma Jaya), dan R.M. Wibawanto Nugroho Widodo, PhD (Wakil Ketua Bidang HANKAM IKAL Strategic Center ISC). *Flyer* acara (a) dan materi presentasi (b) yang disampaikan oleh Feliks Prasepta Sejahtera Surbakti, S.T., M.T., PhD, ditampilkan pada Gambar 1. Acara ini melibatkan koordinasi dengan seluruh pembicara, moderator, dan peserta, yang terdiri dari masyarakat umum. Mayoritas peserta merupakan konstituen Kresna Dewanata Phrosakh, yang mewakili Daerah Pemilihan Jawa Timur 5, meliputi Kabupaten Malang, Kota Batu, dan kota Malang. Webinar dilaksanakan secara daring melalui Zoom. Panitia mengirimkan tautan Zoom kepada peserta yang telah mendaftar sehari sebelum acara. Selain itu, acara ini juga disiarkan langsung melalui saluran YouTube Studio Intel Pasar Minggu. Pada fase pelaksanaan, dilakukan pula evaluasi, termasuk *pre-test* dan *post-test* untuk mengukur perubahan pengetahuan dan kesadaran masyarakat sebelum dan sesudah acara webinar.

Hasil dan Pembahasan

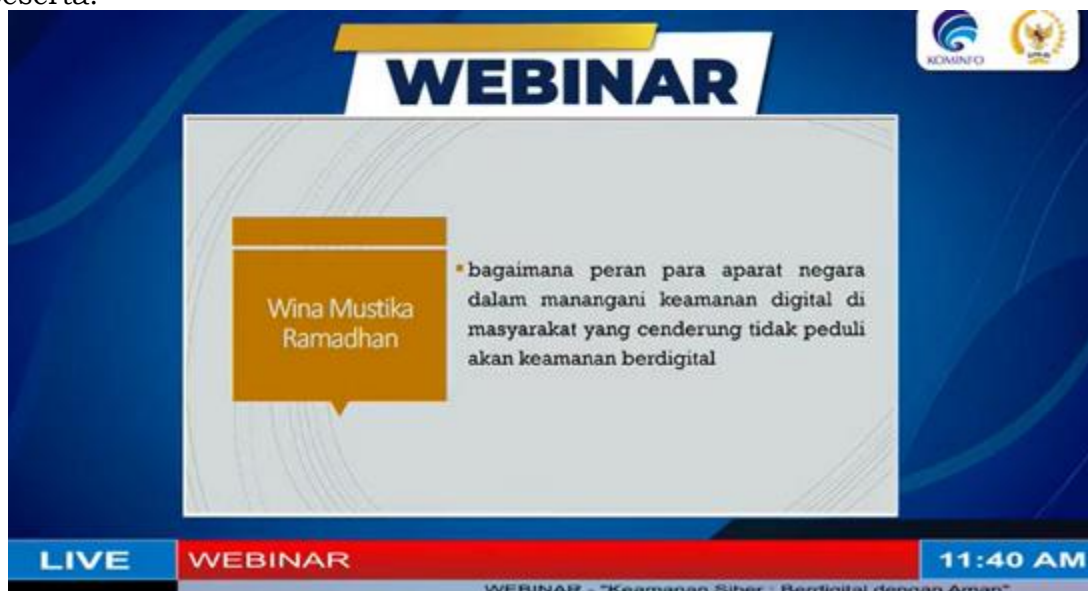
Hasil dari program pengabdian masyarakat "Keamanan Siber: Berdigital dengan Aman" berikut, dilaporkan berdasarkan tahapan yang telah dijelaskan pada bagian metode, yaitu perencanaan, pelaksanaan, dan evaluasi. Pada tahap perencanaan, dilakukan analisis kebutuhan peserta melalui survei awal untuk mengidentifikasi tingkat literasi keamanan digital masyarakat. Survei menunjukkan bahwa lebih dari 60% responden belum memahami ancaman seperti *phishing*, *pharming*, dan *sniffing*. Sebagai respons, materi edukasi dirancang mencakup pengenalan ancaman siber, perlindungan perangkat, dan pengamanan identitas digital. Alat bantu visual berupa infografis dan video pendek disiapkan untuk mempermudah pemahaman peserta, sesuai dengan temuan Hasya et al. (2024) yang menekankan pentingnya alat bantu visual dalam meningkatkan literasi digital. Selain itu, *pre-test* dan *post-test* dirancang untuk mengukur perubahan pemahaman peserta sebelum dan sesudah program.

Hasil utama dari kegiatan pengabdian masyarakat ini adalah terselenggaranya webinar nasional dengan tema "Keamanan Siber: Berdigital dengan Aman" yang diikuti oleh mayoritas peserta dari daerah pemilihan Jawa Timur 5. Peserta acara sebagian besar merupakan konstituen dari Bapak Kresna Dewanata Phrosakh, anggota Komisi I DPR RI. Webinar ini dihadiri oleh 120 peserta dan disiarkan langsung melalui platform Zoom (Gambar 2, 3 dan 4). Sebagai salah satu pembicara utama, penulis juga memberikan presentasi dengan judul "Keamanan Siber: Berdigital dengan Aman" Selain melalui Zoom, acara ini juga tersedia untuk ditonton melalui kanal YouTube yang dikelola oleh Studio Intel Pasar Minggu, dan dapat diakses melalui tautan berikut: <https://www.youtube.com/watch?v=hLa8JCOMzBs&t=3721s>.



Gambar 2. Menyampaikan materi dalam webinar nasional

Pelaksanaan program "Keamanan Siber: Berdigital dengan Aman" menghasilkan peningkatan pemahaman peserta terkait keamanan digital yang terlihat dari hasil *pre-test* dan *post-test*. Pada *pre-test*, rata-rata peserta hanya memiliki pemahaman dasar terkait ancaman siber dan metode pengamanannya. Setelah mengikuti rangkaian kegiatan, *post-test* menunjukkan adanya peningkatan pemahaman yang signifikan, di mana lebih dari 80% peserta mampu mengenali jenis ancaman siber seperti *phishing*, *pharming*, dan *sniffing*, serta metode pencegahan dasar yang dapat mereka terapkan. Data ini menunjukkan bahwa edukasi langsung melalui lokakarya interaktif efektif dalam meningkatkan kesadaran dan pemahaman peserta.



Gambar 3. Pertanyaan dari peserta webinar nasional



Gambar 4. Tampilan screenshot peserta

Selain peningkatan pemahaman tentang ancaman siber, hasil menunjukkan perubahan perilaku dalam penggunaan perangkat digital. Berdasarkan survei pasca-kegiatan, sebanyak 70% peserta menyatakan telah memperbarui kata sandi dengan kombinasi yang lebih kuat, mengaktifkan autentikasi dua faktor, dan menggunakan fitur keamanan perangkat seperti "Find My Device". Ini menunjukkan bahwa peserta tidak hanya memahami konsep keamanan, tetapi juga menerapkannya dalam aktivitas digital mereka sehari-hari. Temuan ini mendukung tujuan awal program, yaitu memberikan solusi praktis yang dapat diterapkan langsung oleh peserta untuk meningkatkan keamanan siber mereka.

Dari sisi pengamanan identitas digital, program ini berhasil meningkatkan kesadaran akan pentingnya menjaga data pribadi. Berdasarkan hasil diskusi kelompok, sebagian besar peserta mengakui bahwa mereka sering membagikan informasi pribadi secara tidak sengaja, seperti nomor telepon atau alamat email di platform publik. Setelah mendapatkan pemahaman dari materi yang disampaikan, lebih dari 70% peserta menyatakan akan lebih berhati-hati dalam membagikan informasi pribadi dan mempertimbangkan pengaturan privasi di media sosial. Hal ini menunjukkan bahwa edukasi mengenai perlindungan identitas digital berhasil meningkatkan kewaspadaan peserta terhadap praktik-praktik yang membahayakan privasi mereka.

Hasil evaluasi juga menunjukkan bahwa studi kasus yang diangkat, seperti kasus peretasan data BPJS dan BRI Life, mampu menarik perhatian peserta dan memperkuat pemahaman mereka mengenai dampak nyata dari kejahatan siber. Studi kasus ini membantu peserta melihat urgensi untuk melindungi data pribadi dan menjaga keamanan perangkat mereka. Dengan contoh kasus yang relevan, peserta lebih termotivasi untuk menerapkan langkah-langkah keamanan siber yang telah dipelajari, yang tercermin dalam hasil survei di mana 85% peserta menganggap topik yang diangkat dalam studi kasus sangat berguna dan memotivasi.

Pembahasan mengenai praktik keamanan perangkat digital juga mendapatkan respon positif. Dari survei pasca-kegiatan, 65% peserta

menyatakan bahwa mereka baru mengetahui beberapa fitur keamanan dasar pada perangkat mereka, seperti otentikasi sidik jari dan aplikasi pencarian perangkat yang hilang. Sebelum mengikuti program ini, banyak peserta yang tidak memanfaatkan fitur-fitur tersebut secara maksimal. Peningkatan pemahaman ini menunjukkan bahwa kegiatan edukasi tidak hanya memberikan informasi baru tetapi juga mendorong pemanfaatan teknologi yang sudah tersedia untuk keamanan pribadi.

Hasil ini konsisten dengan teori literasi digital yang dikemukakan oleh Herawati et al. (2024), yang menyatakan bahwa edukasi berbasis interaksi dapat secara signifikan meningkatkan kesadaran peserta terhadap risiko siber. Penekanan pada pendekatan interaktif, seperti simulasi penggunaan alat keamanan, terbukti efektif dalam memperkuat pemahaman peserta, sebagaimana didukung oleh temuan Daeng et al. (2023) mengenai pentingnya metode praktis dalam edukasi keamanan digital. Selain itu, perubahan perilaku yang dilaporkan oleh peserta mendukung temuan Sidiq (2024), yang menyebutkan bahwa literasi digital tidak hanya meningkatkan kesadaran, tetapi juga mendorong penerapan praktik digital yang lebih aman. Peningkatan kewaspadaan terhadap privasi data yang diakui oleh lebih dari 70% peserta juga relevan dengan kajian Algamar & Ampri (2022) tentang perlindungan jejak digital sebagai mitigasi risiko privasi.

Dibandingkan dengan PKM Herawati et al. (2024) yang berfokus pada siswa SMA, program ini berhasil menjangkau masyarakat umum dengan pendekatan yang lebih inklusif. Pendekatan interaktif melalui webinar dan simulasi alat keamanan memberikan nilai tambah dibandingkan PKM tersebut, yang lebih mengandalkan modul dan diskusi kelompok. PKM Sidiq (2024), yang menekankan etika bermedia sosial, menunjukkan keberhasilan dalam membangun kesadaran peserta terhadap rekam jejak digital. Namun, program kami memperluas cakupan dengan mencakup ancaman teknis, seperti phishing dan pharming, sehingga memberikan pemahaman yang lebih komprehensif. Dibandingkan dengan PKM Daeng et al. (2023) yang menyasar pelaku UMKM, program ini menawarkan solusi praktis untuk individu yang menggunakan teknologi digital dalam kehidupan sehari-hari. Hasil survei menunjukkan bahwa peserta program kami tidak hanya memahami ancaman digital, tetapi juga mampu menerapkan strategi perlindungan dengan segera.

Secara keseluruhan, program ini berhasil mencapai tujuan utama, yaitu meningkatkan literasi keamanan siber di kalangan masyarakat. Peningkatan pemahaman dan perubahan perilaku yang ditunjukkan peserta membuktikan bahwa program edukasi keamanan siber sangat relevan dan diperlukan. Berdasarkan hasil dan pembahasan ini, disarankan agar program serupa dilakukan secara berkala dan menjangkau lebih banyak masyarakat. Hal ini penting mengingat kejahatan siber yang semakin kompleks, sehingga diperlukan pembaruan pengetahuan secara rutin untuk menghadapi berbagai ancaman digital yang terus berkembang.

Simpulan dan Tindak Lanjut

Program pengabdian masyarakat dan bentuk webinar "Keamanan Siber: Berdigital dengan Aman" secara keseluruhan berhasil mencapai tujuan utamanya, yaitu meningkatkan literasi keamanan siber di kalangan masyarakat umum. Melalui pendekatan edukasi yang interaktif dan relevan, peserta tidak hanya memperoleh pemahaman yang lebih baik tentang ancaman siber, tetapi juga mampu mengaplikasikan langkah-langkah pengamanan digital dalam kehidupan sehari-hari. Edukasi ini membantu

masyarakat menjadi lebih bijak dalam penggunaan teknologi digital, serta meningkatkan kewaspadaan mereka terhadap risiko keamanan yang mungkin terjadi. Dengan pencapaian ini, program pengabdian masyarakat ini telah memberikan kontribusi positif dalam menciptakan masyarakat digital yang lebih aman.

Kesimpulan yang dapat diambil dari kegiatan pengabdian masyarakat ini adalah bahwa edukasi keamanan siber berperan penting dalam mencegah dampak negatif dari kejahatan digital. Peningkatan pengetahuan dan perubahan perilaku peserta menunjukkan bahwa masyarakat dapat diberdayakan untuk melindungi data pribadi dan identitas mereka dengan metode yang sederhana namun efektif. Dengan demikian, upaya edukasi seperti ini perlu terus dilakukan untuk menjaga agar masyarakat tetap memiliki kesadaran yang tinggi terhadap ancaman siber yang terus berkembang seiring kemajuan teknologi.

Sebagai tindak lanjut, disarankan agar program edukasi keamanan siber ini dikembangkan lebih lanjut untuk mencakup topik-topik yang lebih mendalam, seperti privasi data, pengamanan untuk usaha kecil, serta pemahaman akan regulasi keamanan data di Indonesia. Edukasi yang lebih mendalam ini akan sangat bermanfaat bagi kelompok masyarakat yang lebih spesifik, seperti pelaku usaha kecil dan mahasiswa, yang berpotensi menjadi target serangan siber. Dengan memperluas cakupan materi, diharapkan lebih banyak masyarakat dapat memperoleh pengetahuan dan keterampilan yang tepat untuk melindungi diri dan bisnis mereka.

Selain itu, kolaborasi dengan institusi pendidikan, perusahaan teknologi, dan pemerintah juga perlu ditingkatkan untuk memperluas jangkauan program edukasi ini. Dengan keterlibatan lebih banyak pihak, program ini bisa menjangkau masyarakat di berbagai wilayah dan latar belakang sosial-ekonomi. Edukasi yang dilakukan secara rutin dan berkesinambungan, serta didukung oleh berbagai pihak, akan memperkuat ketahanan digital masyarakat Indonesia dan mendukung terciptanya ekosistem digital yang lebih aman.

Daftar Pustaka

- Abdullah, M. S., & Ikasari, I. H. (2023). Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan. *JRIIN: Jurnal Riset Informatika dan Inovasi*, 1(1), 96-98.
- Algamar, M. D., & Ampri, A. I. I. (2022). Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak Dari Bahaya Deepfake. *Jurnal Yustika: Media Hukum Dan Keadilan*, 25(01), 25-39.
- Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., Imanuel, S., & Virgio, V. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia. *Innovative: Journal Of Social Science Research*, 3(6), 1135-1145.
- Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, 4(2), 23-31.
- Gandrova, S., & Banke, R. (2023). Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya Deepfake. *Madani: Jurnal Ilmiah Multidisiplin*, 1(10), 21-35.
- Hasya, D. K., Safitri, D., Putra, D. R., Maulana, F. B. G., & Rakhmawati, N. A. (2024). Implikasi Etika dalam Profil dan Strategi Penipuan Online

- dalam Transaksi e-Commerce di Ranah Cybercrime. *Jurnal Manajemen Riset Inovasi*, 2(1), 236-247.
- Herawati, E. S. B., Mustofa, Z., Sari, M. N., Mirsa, N. R. P., Widiyan, A. P., & Astuti, Y. (2024). Edukasi Digital Safety Dalam Meningkatkan Kecakapan Bermedia Digital Siswa. *Lamahu: Jurnal Pengabdian Masyarakat Terintegrasi*, 3(1), 47-54.
- Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, 8(2), 137-144.
- Kasim, F. M., Daud, M., Mursalin, M., & Ali, M. (2022). Pembinaan Masyarakat Melalui Edukasi Bahaya Pinjaman Online Untuk Menghindari Bahaya Kejahatan Siber di Gampong Cot Keumuneng Kecamatan Sawang Kabupaten Aceh Utara. *Jurnal Solusi Masyarakat Dikara*, 2(3), 158-165.
- Krisnaningsih, E., Dwiyatno, S., Jubaedi, A. D., & Shafitri, A. (2023). Increasing Ethical Understanding of the Use of Information Technology Through Digital Literacy Proficiency Training. *Dinamisia: Jurnal Pengabdian Kepada Masyarakat*, 7(3), 789-801.
- Marwati, F., & Astofa, A. (2024). Pentingnya Edukasi Cyber Security Untuk Menjaga Keamanan Data Pribadi dari Serangan Cyber Phishing Bagi Siswa/Siswi PKBM INTAN Tangerang Selatan. *AMMA: Jurnal Pengabdian Masyarakat*, 2(12: Januari), 1508-1514.
- Nasrudin, F. K., & Latumahina, R. E. (2022). Perlindungan Hukum Terhadap Konsumen Kartu Sim Yang Mengalami Kebocoran Data Akibat Peretasan. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 2(1), 331-343.
- Prasetya, W., & Surbakti, F. P. (2023). Pelaksanaan Kegiatan Pengabdian Masyarakat Webinar Nasional Building Bright Future for Generation Z bagi Siswa-Siswi SMA Jabodetabek. *Jurnal Pengabdian Masyarakat Charitas*, 3(02), 45-52.
- Putri, B. A., Fadilla, D. I., Firdaus, L., Amalia, R. P. D., Ginting, R. A., & Yuspin, W. (2023). Analisis Yuridis Resiko Program Pembukaan Rekening Digital tanpa Buku Rekening Fisik terhadap Kehilangan Telepon Pintar. Prosiding Seminar Nasional Program Doktor Ilmu Hukum,
- Rahma, S. D., Putra, B. A., & Djarwadi, L. F. (2023). Analysis of the Indonesian Government's Efforts in Overcoming Public Data Leak Cases. Proceedings of Sunan Ampel International Conference of Political and Social Sciences,
- Saputra, A., Wijoyo, A., Pratama, M. R. A., & Rahman, R. (2023). Analisis Serangan Phising dan Strategi Deteksinya. *JRIIN: Jurnal Riset Informatika dan Inovasi*, 1(4), 17-31.
- Saputri, V. D. (2023). Implementation Of Biometric-Based Security System On Mobile Banking Application. *Jurnal Komputer Indonesia*, 2(1), 25-32.
- Sari, S. D. (2023). Privasi dan Keamanan Data Dalam Statistik Resmi: Tantangan dan Solusi Dalam Perlindungan Data Individu. *Madani: Jurnal Ilmiah Multidisiplin*, 1(11), 71-83.
- Sidiq, P. (2024). Literasi Digital Pada Masyarakat: Etis Bermedia Sosial, Aman dan Nyaman. *Jurnal Pengabdian Literasi Digital Indonesia*, 3(2), 89-96.

- Surbakti, F. P. S. (2024). Edukasi Tantangan Transformasi Digital di Dunia Bisnis pada Masyarakat Dapil Sumatera Selatan 2. *Jurnal Abdimas Ekonomi dan Bisnis*, 4(2), 175-182.
- Tarigan, E. K., Darmayanti, E., Kartika, F. B., Yani, F., & Salsabila, J. (2024). Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Syarat Dan Ketentuan Aplikasi Online E-Commerce Di Desa Percut Sei Tuan. *JUDIMAS*, 5(1), 32-45.
- Yel, M. B., & Nasution, M. K. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama (JIK)*, 6(1), 92-101.