

DETEKTIF DIGITAL: MELATIH SDN GISIK CEMANDI SIDOARJO MELINDUNGI DATA PRIBADI DAN KESEHATAN

DIGITAL DETECTIVES: TRAINING SDN GISIK CEMANDI SIDOARJO TO PROTECT PERSONAL AND HEALTH DATA

Agustinus Setiono^{*}, Anna Rosarini, Rustandi

STIKES Hang Tuah Surabaya, Surabaya, Indonesia

^{*}e-mail: agustinus@stikeshangtuah-sby.ac.id

Received 2026-06-29

Revised 2026-08-06

Accepted 2026-08-07

Published 2026-08-12

Abstrak

Pengabdian kepada Masyarakat (PKM) ini dilatarbelakangi tingginya penggunaan gawai oleh anak sekolah dasar tanpa pemahaman literasi digital, sehingga rentan penyalahgunaan data pribadi dan informasi kesehatan. PKM bertujuan meningkatkan kesadaran siswa SDN Gisik Cemandi Sidoarjo dalam melindungi data sensitif di dunia maya. Metode pelaksanaan menggunakan pelatihan interaktif berkonsep "Detektif Digital", meliputi pemaparan materi multimedia, simulasi kasus pada permainan *Mobile Legends* dan *Roblox*, serta permainan peran. Hasil kegiatan menunjukkan peningkatan signifikan pemahaman siswa mengenai jenis data pribadi yang wajib dilindungi, seperti nama lengkap, alamat, dan riwayat kesehatan. Sebelum pelatihan, hanya 35% siswa yang memahami risiko berbagi data di internet, namun pascapelatihan angka tersebut melonjak menjadi 88%. Siswa juga mampu mengidentifikasi ancaman siber sederhana secara mandiri. Kesimpulannya, pendekatan edukasi tematik interaktif "Detektif Digital" sangat efektif menanamkan budaya menjaga privasi digital sejak dini. Keberlanjutan kegiatan dimasa depan memerlukan dukungan dan pengawasan aktif dari guru serta orang tua di rumah sebagai detektif digital.

Kata Kunci: detektif digital; data pribadi; kesehatan; perlindungan; SDN Gisik Cemandi

Abstract

*This Community Service (PKM) programme stems from the high rate of gadget use among primary school pupils lacking digital literacy skills, which leaves them vulnerable to the misuse of personal data and health information. The initiative aimed to enhance awareness among pupils at SDN Gisik Cemandi Sidoarjo in protecting sensitive online data. The implementation method utilised interactive training based on a "Digital Detective" concept, incorporating multimedia presentations, case simulations within *Mobile Legends* and *Roblox*, and role-playing exercises. Findings revealed a significant improvement in pupils' comprehension of confidential personal data needing protection, such as full names, home addresses, and medical histories. Prior to the training, only 35% of pupils recognised the risks of sharing data on the internet, whereas post-*

1128



training this figure surged to 88%, with pupils demonstrating the ability to independently identify basic cyber threats. In conclusion, the interactive thematic approach of the "Digital Detective" programme is remarkably effective in instilling a culture of digital privacy from a young age. Moving forward, the future sustainability of these activities will rely heavily on active support and supervision from both teachers and parents at home acting as digital detectives.

Keywords: *digital detective; Gresik Cemandi elementary school; health; protect; personal data*

PENDAHULUAN

Perkembangan teknologi informasi dan teknologi digital telah mengubah lanskap interaksi anak-anak usia sekolah dasar, bertransformasi dari sekadar media hiburan menjadi ruang belajar dan bersosialisasi yang tak terpisahkan. Namun, intensitas penggunaan gawai yang tinggi ini tidak dibarengi dengan kemampuan literasi digital yang memadai, khususnya dalam aspek keamanan siber (*cybersecurity*) (Slamet et al., 2026). Anak-anak merupakan kelompok yang paling rentan terhadap kejahatan digital karena anak-anak belum mampu mengetahui dan memahami informasi yang sensitif dan rahasia di platform media sosial atau *game online* (seperti *Roblox* dan *Mobile Legends*) (Wilbanks, 2021). Data rentan tersebut meliputi nama lengkap, nomor telepon orang tua, hingga data kesehatan (seperti kondisi fisik atau riwayat penyakit). Tanpa adanya pemahaman tentang jejak digital (*digital footprint*), data ini rawan dieksploitasi untuk tindakan kriminal seperti pencurian identitas, perundungan siber (*cyberbullying*), hingga manipulasi psikologis (*social engineering*) (Zaman et al., 2024). Di lingkungan sekolah pun kurikulum sekolah formal dan kurangnya pengawasan orang tua dalam memberikan edukasi proteksi data yang terstruktur. Di SDN Gisik Cemandi Sidoarjo, yang terletak di kawasan pesisir dengan akses internet merata, mitigasi preventif sangat mendesak dilakukan mengingat mayoritas siswa aktif di dunia maya namun belum memiliki kesadaran siber (*cyber awareness*) dasar (Surya et al., 2024).



Beberapa kegiatan pengabdian kepada masyarakat (PKM) terdahulu memiliki fokus kegiatan dengan tema literasi digital bagi anak usia sekolah dasar. Namun, mayoritas program literasi digital yang ada masih bersifat umum, seperti edukasi penggunaan internet sehat secara makro, pengenalan perangkat keras dan lunak, atau pencegahan kecanduan gawai (*gadget addiction*) (AlHidaifi et al., 2024; Bharati, 2024; Lusiana & Nugroho, 2024). Metode penyampaian yang digunakan pada PKM konvensional umumnya mengandalkan komunikasi satu arah seperti ceramah, pembagian pamflet, atau presentasi searah yang cenderung teoritis, teknis, dan membosankan bagi anak-anak. Fokus perlindungan data pribadi dalam literasi digital sarannya masih sering ditujukan kepada remaja atau orang dewasa, sementara anak-anak sekolah dasar kerap kali diabaikan atau hanya dianggap sebagai objek pengawasan orang tua, bukan sebagai agen aktif yang memegang kendali atas datanya sendiri.

Kebaruan (*novelty*) dari kegiatan PKM ini menggabungkan tiga aspek yang membedakannya dengan kegiatan literasi digital lainnya diantaranya fokus spesifik pada Data Kesehatan, berbeda dengan PKM literasi digital lain yang hanya melindungi data identitas umum (KTP/Kartu Keluarga), kegiatan ini secara khusus mengintegrasikan edukasi terhadap perlindungan data pribadi sekaligus data informasi kesehatan (seperti riwayat penyakit, rekam medis sederhana, dan kondisi fisik) sejak usia dini, relevan dengan kepakaran pelaksana kegiatan PKM yaitu dalam bidang Manajemen Informasi Kesehatan. Kedua, pendekatan gamifikasi tematik Detektif Digital (Kuss et al., 2012), PKM ini memberikan informasi, pengetahuan tentang materi keamanan siber yang perlu menjadi sebuah petualangan interaktif bagi generasi muda. Siswa bukan sebagai pendengar pasif, melainkan aktif ikut andil dalam pelatihan ini dan dibekali ID Card fisik untuk memecahkan kasus kebocoran data yang dipraktikkan dalam *game* favorit mereka (*Mobile Legends* dan *Roblox*). Ketiga, menggunakan metode bermain peran (*Role-Playing*) berbasis Kinestetik sebagai dasar edukasi yang melibatkan gerakan tubuh,



analisis berkas misteri siber, dan simulasi penolakan *phishing*, sehingga mempercepat retensi informasi melalui emosi positif anak (Arisanty et al., 2025; Slamet, 2025).

Kegiatan ini menggunakan model pembelajaran dengan metode edukasi tematik-interaktif yang dapat diadopsi oleh guru untuk mengintegrasikan materi literasi digital dan keamanan data ke dalam kegiatan ekstra kurikuler sekolah secara berkelanjutan (Rahmawati et al., 2024; Sudarmo et al., 2021). Bagi Orang Tua, dapat membantu meringankan beban pengawasan digital dengan membentuk karakter anak yang agar lebih memahami siber, sehingga anak mampu menyaring secara mandiri informasi yang boleh dan tidak boleh dibagikan ke publik. Dan bagi Keilmuan / Tim PKM, menerapkan kemampuan dalam bidang Manajemen Informasi Kesehatan dalam aspek preventif-komunitas, serta menambah literatur mengenai efektivitas gamifikasi dalam pengajaran *cybersecurity* untuk anak-anak (Hartati et al., 2022; Yunus & Syukur, 2025).

Tujuan Kegiatan, untuk meningkatkan kesadaran (*cyber awareness*) dan pemahaman bagi siswa SDN Gisik Cemandi Sidoarjo mengenai jenis data pribadi dan data kesehatan yang bersifat rahasia yang wajib melindungi diri di dunia maya. Melatih keterampilan siswa dalam mengidentifikasi potensi ancaman siber sederhana (seperti tautan *phishing*, akun palsu, atau modus penipuan berhadiah di dalam gim). Mengubah perilaku siswa agar lebih bertanggung jawab, cerdas, dan preventif dalam mengelola aktivitas digital serta menjaga privasi mereka sejak dini (Utami et al., 2026). Sedangkan manfaat kegiatan diharapkan, bagi Siswa SDN Gisik Cemandi, Siswa memperoleh pengetahuan proteksi siber secara aplikatif dan menyenangkan, sehingga memiliki kemampuan proteksi mandiri dari risiko eksploitasi data, peretasan akun *game* maupun kejahatan siber lainnya di internet.

METODE

Kegiatan Pengabdian kepada Masyarakat (PKM) ini dilaksanakan di SDN Gisik Cemandi, Kecamatan Sedati, Kabupaten Sidoarjo, pada tanggal 11 Juni 2026, dengan sasaran untuk siswa-siswi kelas atas (kelas 4, 5, dan 6) sebanyak 45 siswa. Pendekatan kegiatan menggunakan pendekatan edukasi tematik interaktif "Detektif Digital" berbasis gamifikasi dengan bermain peran untuk menanamkan kesadaran serta budaya perlindungan data pribadi siswa sejak dini. Pendekatan pelaksanaan program dirancang secara terstruktur melalui empat tahapan utama: Tahap Perencanaan/Persiapan, Tahap Pelaksanaan, Tahap Evaluasi, dan Tahap Monitoring & Evaluasi (Monev), diantaranya :

Tahap Perencanaan (Persiapan), tahap ini sebagai dasar untuk memastikan program berjalan dengan baik dan tepat sasaran. Aktivitas pada tahap ini meliputi: Observasi dan Wawancara : Tim PKM melakukan koordinasi dengan Kepala Sekolah dan perwakilan guru SDN Gisik Cemandi untuk melakukan pemetaan potensi, durasi penggunaan internet, *platform game* yang sering dimainkan termasuk *Mobile Legends* dan *Roblox*, serta mengidentifikasi belum adanya kurikulum literasi keamanan data di sekolah tersebut. Penyusunan Modul dan Media Edukasi: Tim menyusun modul khusus bertema "Detektif Digital" yang mengemas materi teknis *cyber security* ke dalam bahasa anak-anak. Atribut pendukung seperti ID Card "Detektif Digital", lembar kasus misteri siber, dan visualisasi multimedia (video animasi pendek) disiapkan pada tahap ini. Penyusunan Instrumen Evaluasi: Mengembangkan draf soal *pre-test* dan *post-test* yang telah divalidasi secara internal oleh pakar Manajemen Informasi Kesehatan.

Tahap Pelaksanaan, pelaksanaan inti PKM menggunakan pendekatan gamifikasi dan *experiential learning* (belajar melalui pengalaman) yang dibagi ke dalam empat sub-agenda: (a) Pengondisian dan *Pre-Test* : Siswa dikondisikan di dalam kelas / aula, diberikan atribut ID Card Detektif untuk memicu keterikatan emosional (*engagement*). Sesi diawali dengan pengerjaan *pre-test* secara mandiri

selama 15 menit. Edukasi Interaktif ("Misi Rahasia") : Penyampaian materi dikonsep sebagai pengarahan misi (mission briefing). Tim memaparkan uraian data menggunakan analogi visual didalamnya terdapat : (a) Data Umum/Publik : Hobi, warna favorit. Data Rahasia/Sensitif: Nama lengkap, alamat, Kartu Keluarga, serta data kesehatan (riwayat sakit, kondisi fisik, rekam medis sederhana). (b) Simulasi Kasus (*Role-Playing*): Siswa dibagi ke dalam 5 kelompok detektif kecil. Setiap kelompok diberikan Lembar Kasus berisi skenario ancaman siber, seperti: (1) Kasus 1: Akun game *Roblox* yang di-hacker akibat memberikan kata sandi ke teman. (2) Kasus 2: Orang asing di dalam *Mobile Legends* yang meminta foto Kartu Keluarga dengan iming-iming diamond gratis (*phishing/social engineering*). (c) Siswa diminta melakukan analisis kesalahan tokoh, mempraktikkan gerakan tubuh penolakan siber, dan mendiskusikan solusinya. (d) Refleksi dan *Post-Test* : Setiap kelompok mempresentasikan berkas perkara yang berhasil dipecahkan, dilanjutkan dengan pengisian post-test akhir.

Tahap Evaluasi, data dalam kegiatan PKM ini dikumpulkan menggunakan dua jenis instrumen utama: (a) Kuesioner Objektif (Kuantitatif) : Berupa lembar soal *pre-test* dan *post-test* yang terdiri dari 10 butir pertanyaan pilihan ganda. Soal mencakup komponen: kognitif data pribadi/kesehatan (4 soal), kesadaran risiko berbagi data (3 soal), dan tindakan preventif siber (3 soal). Lembar Observasi Terstruktur (Kualitatif): Digunakan oleh tim pengabdian untuk menilai keaktifan siswa, kemampuan penalaran kritis saat *role-play*, serta ketepatan siswa dalam mengambil keputusan saat simulasi pemecahan kasus. (b) Analisis Data dengan Analisis Kuantitatif, data nilai *pre-test* dan *post-test* diolah menggunakan teknik statistik deskriptif. Nilai dihitung berbasis persentase ketepatan jawaban total siswa sebelum dan sesudah intervensi guna melihat gain score (peningkatan pemahaman).

$$\text{Persentase Pemahaman} = \frac{\text{Jumlah Jawaban Benar}}{\text{Total Soal}} \times 100\%$$



(c) Analisis Kualitatif : Data hasil observasi dan umpan balik (*feedback*) dari guru pendamping dianalisis secara naratif-deskriptif untuk menggambarkan perubahan perilaku dan antusiasme psikomotorik siswa selama kegiatan. (d) Indikator Keberhasilan Evaluasi, Program PKM ini dinyatakan berhasil apabila memenuhi indikator capaian berikut:

Tabel 1 Komponen Evaluasi

No	Komponen Evaluasi	Target Capaian Kuantitatif / Kualitatif
1	Peningkatan Kognitif	Minimal 75% dari total peserta mengalami peningkatan nilai dari pre-test ke post-test, dengan rata-rata nilai post-test ≥ 80 .
2	Keterampilan Psikomotorik	Minimal 80% kelompok detektif mampu mengidentifikasi celah keamanan siber dan merumuskan mitigasi pada lembar kasus dengan tepat.
3	Kepuasan Mitra	Guru pendamping memberikan respons positif (kategori "Sangat Baik") terhadap relevansi metode "Detektif Digital".

HASIL DAN PEMBAHASAN

Kegiatan Pengabdian Kepada Masyarakat (PKM) dengan tema "Detektif Digital" telah dilaksanakan pada tanggal 11 Juni 2026 dengan sukses di SDN Gisik Cemandi Sidoarjo. Kegiatan ini diikuti 45 siswa yang berasal dari perwakilan kelas 4, 5 dan 6. Pemilihan kelompok usia ini didasarkan pada hasil observasi awal yang menunjukkan bahwa mereka berada pada fase transisi di mana intensitas penggunaan perangkat elektronik sebagai media komunikasi dan internet untuk media sosial dan game online mulai meningkat pesat, namun belum dibekali dengan proteksi literasi digital yang memadai.

Pelaksanaan program berjalan sesuai dengan rancangan metode yang telah ditetapkan. Pada awal sesi, para siswa diberikan atribut berupa ID Card "Detektif Digital" untuk membangun atmosfer belajar yang mengikuti keadaan dan kondisi serta menyenangkan saat praktik dilapangan. Penyampaian materi dikemas melalui



analogi "Misi Rahasia", di mana siswa diajarkan untuk mengklasifikasikan informasi mana yang bersifat umum dan informasi mana yang bersifat rahasia (data pribadi dan data kesehatan).

Tabel 2 Kategori Data Pribadi

No	Kategori Data Pribadi & Kesehatan	Status Kerahasiaan (Edukasi PKM)	Contoh Kasus yang Disimulasikan
1	Nama lengkap, alamat rumah, nomor HP	Sangat Rahasia	Orang asing di games daring meminta alamat rumah untuk mengirim hadiah.
2	Riwayat penyakit, kondisi fisik, rekam medis	Saras / Rahasia	Mengunggah foto saat sakit di media sosial dengan detail lokasi rumah sakit.
3	Kartu Identitas Anak (KIA) / KK	Sangat Rahasia	Mengikuti kuis daring yang meminta foto identitas diri.
4	Hobi, warna favorit, makanan kesukaan	Publik / Umum	Berbagi cerita mengenai hobi membaca di forum ramah anak.

Melalui simulasi berbasis kasus pada Tabel 2, siswa diajak melakukan role-playing dalam 5 kelompok kecil untuk membedahkan berkas kasus "Pencurian Identitas Digital". Siswa berhasil melatih penalaran kritis dengan mengidentifikasi celah siber seperti bahaya mengeklik tautan phishing palsu dan pentingnya membuat kata sandi (*password*) yang kuat dan unik serta dan merumuskan langkah mitigasinya, seperti membuat kata sandi yang kuat dan menolak permintaan data dari akun tidak dikenal.

Untuk mengukur efektivitas metode "Detektif Digital" dalam meningkatkan pemahaman siswa mengenai perlindungan data pribadi dan kesehatan, dilakukan analisis komparatif terhadap nilai *pre-test* dan *post-test*. Instrumen evaluasi terdiri dari 10 pertanyaan pilihan ganda terkait pemahaman jenis data sensitif, risiko membagikan data, dan tindakan preventif saat menghadapi ancaman siber.

Sebelum intervensi program dilakukan (*pre-test*), tingkat pemahaman siswa hanya berada pada rata-rata 35%. Sebagian besar siswa menganggap bahwa membagikan nama lengkap, nomor telepon, dan kondisi kesehatan di *platform*



digital (seperti bio media sosial atau ruang obrolan gim) adalah hal yang aman dan lumrah. Mereka belum menyadari konsep jejak digital (*digital footprint*) yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan penipuan (*social engineering*).

Tabel 3 Hasil Evaluasi

No	Parameter Evaluasi	Sebelum Pelatihan (<i>Pre-Test</i>)	Setelah Pelatihan (<i>Post-Test</i>)	Selisih Peningkatan	Status Capaian
1	Rata-Rata Nilai / Tingkat Pemahaman	35%	88%	+53%	Sangat Baik (Melampaui Target $\geq 80\%$)
2	Estimasi Jumlah Siswa yang Kompeten	± 16 Siswa	± 40 Siswa	+24 Siswa	Kenaikan Signifikan
3	Pemahaman Jejak Digital (Digital Footprint)	Rendah (Menganggap aman membagikan no. HP & bio)	Tinggi (Sadar bahaya social engineering)	Perubahan Persepsi	Berhasil Diintervensi
4	Kemampuan Mitigasi Ancaman Siber	Pasif / Bingung	Aktif (Mampu mendeteksi phishing & mengunci akun)	Peningkatan Keterampilan	Berhasil Diintervensi

Setelah rangkaian pelatihan interaktif selesai dilaksanakan (*post-test*), tingkat pemahaman siswa meningkat mencapai 88%. Siswa memiliki kesadaran yang mampu membedakan data yang boleh dipublikasikan dan dengan data yang wajib dilindungi. Kemampuan penalaran kritis siswa juga terasah melalui metode studi kasus, di mana mereka tidak lagi sekadar menghafal teori, tetapi memahami mengapa data tersebut berbahaya jika jatuh ke tangan yang salah.

Analisis keberhasilan metode dengan menggunakan pendekatan tematik Detektif Digital efektif memotong kekakuan materi keamanan siber. Berdasarkan



teori pembelajaran anak, metode bermain peran (*role-playing*) dan gamifikasi mempercepat retensi informasi karena melibatkan emosi positif dan keterlibatan aktif siswa secara langsung, berbeda dengan metode ceramah konvensional yang cenderung membosankan bagi anak usia sekolah dasar. Dan kegiatan PKM ini telah dilakukan dengan memberikan ilmu dan pengetahuan sebagai dasar *cyber awareness* pada siswa SDN Gisik Cemandi. Perubahan perilaku ini diharapkan dapat meminimalkan risiko eksploitasi data anak di wilayah Sidoarjo, khususnya di lingkungan mitra.

Analisis dalam perspektif kualitatif, dengan melakukan evaluasi berbasis observasi selama rangkaian kegiatan serta refleksi *pre-test* dan *post-test* menunjukkan adanya perubahan dan transformasi yang mendasar pada aspek afektif, kognitif, dan psikomotorik siswa. Sebelum pelatihan (*pre-test*), siswa cenderung bersikap pasif dan menganggap aman tindakan membagikan data sensitif seperti nama lengkap, nomor HP, maupun riwayat kesehatan di *platform game* karena belum memahami risiko dalam jejak digital (*digital footprint*) dan manipulasi psikologis (*social engineering*) dalam media sosial.

Tabel 4 Aspek Observasi dalam Kegiatan

Aspek Observasi	Kondisi Awal (<i>Pre-Test</i>)	Kondisi Akhir (<i>Post-Test</i>)	Perubahan Perilaku
Sikap & Kesadaran Privasi	Pasif dan acuh; menganggap wajar membagikan identitas diri di kolom obrolan game.	Aktif dan mitigatif; menyadari kerahasiaan data pribadi serta risiko eksploitasi siber.	Bertransformasi menjadi agen aktif yang memegang kendali proteksi atas datanya sendiri.
Penalaran Kritis & Analisis Ancaman	Bingung dan tidak mampu mendeteksi adanya indikasi kejahatan siber sederhana.	Mampu mengidentifikasi modus phishing, akun palsu, dan iming-iming diamond gratis pada akun.	Terasah melalui analisis berkas kasus misteri siber pada skenario gim favorit.



Tindakan Psikomotorik / Mitigasi	Rentan menyerahkan kata sandi atau data keluarga kepada orang tidak dikenal.	Mampu membuat kata sandi yang kuat/unik dan memperagakan simulasi penolakan siber secara langsung.	Terbentuk melalui latihan gerakan kinestetik dan simulasi <i>role-playing</i> kelompok.
Antusiasme Pembelajaran	Cenderung cepat bosan jika materi disampaikan melalui ceramah yang kaku dan teoritis.	Terlibat penuh, bisa mengikuti dalam keadaan tertentu, dan menunjukkan energi dan emosi positif selama memegang sebagai "Detektif Digital".	Pendekatan tematik gamifikasi berhasil mengurangi kekakuan penyampaian materi keamanan siber yang teknis

Selama pelaksanaan, penggunaan metode bermain peran (*role-playing*) berbasis gamifikasi kinestetik, memiliki hasil yang mampu membangkitkan emosi positif dan antusiasme tinggi, di mana siswa secara aktif berdiskusi dalam kelompok untuk memecahkan simulasi kasus kebocoran data pada game *Roblox* dan *Mobile Legends*. Pascapelatihan (*post-test*), perubahan perilaku terlihat hasil dari adanya pergeseran pola pikir siswa menjadi aktif-mitigatif, yang ditandai dengan memiliki kemampuan nalar secara kritis dalam mengenali indikasi tautan *phishing*, mempraktikkan dan memperagakan simulasi penolakan ancaman siber, serta mampu membedakan data publik dan data rahasia secara mandiri.

Dokumentasi kegiatan yang disajikan pada Gambar 1 yang secara visual merekam seluruh rangkaian intervensi berbasis *experiential learning* dan gamifikasi yang diikuti oleh siswa SDN Gisik Cemandi Sidoarjo. Rangkaian foto tersebut memperlihatkan tiga fase dalam pelaksanaan program, dimulai dari pembagian atribut fisik berupa ID Card "Detektif Digital" untuk membangun atmosfer belajar yang imersif, kedinamisan diskusi kelompok kecil saat para siswa menganalisis berkas kasus misteri siber (*Roblox* dan *Mobile Legends*) secara kritis, hingga sesi penyerahan komitmen literasi digital secara simbolis sebagai wujud konkrit penanaman budaya privasi.





Gambar 1 Kegiatan Detektif Digital

Gambar 1 menjadi bukti kegiatan dilapangan bahwa keterlibatan aktif dan metode bermain peran (*role-playing*) mampu memotong kekakuan materi keamanan siber yang teknis, menciptakan emosi positif, serta merangsang interaksi kinestetik anak-anak, yang pada akhirnya berkontribusi langsung terhadap lonjakan signifikan pemahaman siber klasikal peserta dari 35% menjadi 88%.

Pembahasan

Keberhasilan intervensi dini melalui metode "Detektif Digital" pada siswa sekolah dasar menguraikan bahwa kesadaran siber perlu dibangun secara berkesinambungan seiring dengan meningkatnya usia anak dan kompleksitas teknologi yang mereka gunakan (Zaman et al., 2024). Ketika anak-anak beranjak remaja menuju fase Generasi Z, khususnya saat menempuh pendidikan di jenjang Sekolah Menengah Atas (SMA), ancaman siber yang dihadapi tidak lagi sebatas peretasan akun *game daring* sederhana, melainkan berbaur menjadi kejahatan teknologi digital yang jauh lebih canggih dan terstruktur (Arisanty et al., 2025; Telekomunikasi, Informatika, Siber, Dan Internet - Informasi Publik, 2018). Level remaja SMA menjadi sangat rentan terhadap eksploitasi data pribadi untuk penipuan finansial, pencurian identitas demi pinjaman *online* ilegal, perundungan siber (*cyberbullying*), hingga manipulasi psikologis (*social engineering*)

1139



(Alabdulkarim et al., 2024; Kuss et al., 2012). Sehingga, hasil positif dari pengabdian masyarakat ini perlu dipandang sebagai dasar untuk merumuskan strategi proteksi data yang lebih progresif, mengingat siswa SMA memiliki mobilitas digital yang sangat tinggi dan jejak digital (*digital footprint*) yang ditinggalkan jauh lebih berisiko bagi keamanan personal maupun keluarga mereka.

Guna mengantisipasi eskalasi kejahatan internet yang menasar anak remaja ini, pemerintah melalui Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi bersama Kementerian Komunikasi dan Digital disarankan untuk segera merumuskan edukasi keamanan siber dan privasi data ke dalam kurikulum wajib tingkat SMA. Pemerintah tidak boleh memperlakukan literasi digital sekadar sebagai materi pengenalan perangkat keras atau perangkat lunak secara umum, melainkan harus mengadopsi model gamifikasi dan studi kasus riil dengan tren kehidupan Generasi Z (Alfan & Wea, 2026). Kebijakan kurikulum masa depan perlu secara eksplisit mengintegrasikan pilar ketahanan siber (*cyber resilience*), pemahaman praktis mengenai Undang-Undang Perlindungan Data Pribadi (UU PDP), etika digital, serta teknik enkripsi data sederhana. Siswa SMA tidak hanya menjadi konsumen teknologi yang pasif, melainkan memiliki kemampuan bernalar kritis untuk mendeteksi bahaya makro di ruang siber secara mandiri.

Selain perubahan kurikulum, pemerintah juga perlu membangun ekosistem digital yang suportif dengan memfasilitasi kolaborasi secara sistematis antara aparat penegak hukum (seperti unit *Cyber Crime Polri*), institusi pendidikan tinggi, dan penyedia platform digital global. Saran bagi pemerintah adalah menyediakan wadah dan kanal pengaduan siber khusus remaja yang bersifat interaktif, ramah anak, dan menjamin kerahasiaan identitas pelapor, sehingga siswa SMA yang menjadi korban kejahatan internet tidak merasa takut atau terstigma saat mencari pertolongan (Soebijono Tony, 2020). Lewat penguatan regulasi yang inklusif serta pelibatan aktif akademisi dalam program pengabdian masyarakat yang terstruktur di tingkat SMA, pemerintah dapat mencetak Generasi Z yang tidak hanya cerdas



secara digital, melainkan juga tangguh dan mampu memitigasi segala bentuk kriminalitas di jagat maya demi mewujudkan kedaulatan digital Indonesia (Anisti, Anisti; Sidara; Veranus; Imran, 2024; Soebijono et al., 2025).

SIMPULAN

Kegiatan pengabdian masyarakat melalui pendekatan edukasi tematik interaktif "Detektif Digital" berbasis gamifikasi dan bermain peran terbukti efektif dalam menanamkan kesadaran serta budaya perlindungan data pribadi maupun kesehatan bagi siswa sejak dini. Kegiatan ini memiliki keterbatasan, seperti jangkauan intervensi yang masih terbatas pada tingkat sekolah dasar dengan penggunaan media modul fisik, serta keberlanjutan pembentukan karakter cerdas siber yang sangat bergantung pada partisipasi dan pengawasan aktif dari guru maupun orang tua di rumah. Sedangkan, future kegiatan atau rencana tindak lanjut dari program ini meliputi pengembangan materi ke tingkat yang lebih kompleks untuk jenjang SMP dan SMA (seperti mitigasi judi online, pinjaman online ilegal, dan perundungan siber), pembentukan kaderisasi "Duta Detektif Digital" sebagai agen edukasi sebaya, serta digitalisasi modul fisik menjadi aplikasi gim seluler atau situs *web* interaktif agar dapat diakses secara mandiri oleh sekolah-sekolah lain di seluruh Indonesia.

UCAPAN TERIMA KASIH

Tim pelaksana kegiatan Pengabdian kepada Masyarakat (PKM) menyampaikan terima kasih sebesar-besarnya kepada LPPM STIKES Hang Tuah Surabaya atas dukungan pendanaan dan administratif, dan kepada pihak SDN Gisik Cemandi Sidoarjo atas perizinan, fasilitas, dan kerja samanya, serta seluruh siswa yang telah berpartisipasi secara antusias sebagai "Detektif Digital".



DAFTAR PUSTAKA

- AlHidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). Towards a Cyber Resilience Quantification Framework (CRQF) for IT infrastructure. *Computer Networks*, 247, 110446. <https://doi.org/10.1016/j.comnet.2024.110446>
- Anisti, Anisti; Sidara; Veranus; Imran, M. S. (2024). Tantangan Literasi Digital Generasi Z: Kajian Sistematis Literature Review. *Media Bahasa, Sastra, Dan Budaya Bahana*, 30(2), 152–161. <https://doi.org/10.33751/wahana.v30i2.11870>
- Arisanty, M., Riady, Y., Kharis, S. A. A., Permatasari, S. M., & Sukatmi, S. (2025). Cerdas Dan Aman Bermedia Digital: Peningkatan Kesadaran Keamanan Siber di Era Hoaks Dan Phishing. *Jurnal Pengabdian Kepada Masyarakat Patikala*, 4(4), 1407–1418.
- Alabdulkarim, N. A., Haq, M. A., & Gyani, J. (2024). Exploring Sentiment Analysis on Social Media Texts. *Engineering, Technology & Applied Science Research*, 14(3), 14442–14450. <https://doi.org/10.48084/etasr.7238>
- Alfan, M. B., & Wea, E. (2026). Analisis Penerimaan Pengguna terhadap Gamifikasi Shopee Games dan Dampaknya pada Perilaku Pembelian Online: Perspektif Technology Acceptance Model (TAM). *Jurnal Ilmiah Sistem Informasi*, 5(2), 334–345. <https://doi.org/10.51903/xegbnc57>
- Bharati, R. K. (2024). Cyber Threats and the Erosion of Privacy: Examining the Delicate Equilibrium. <https://doi.org/10.20944/preprints202407.1577.v1>
- Fan, Z., An, Y., Zhao, H., & Peng, H. (2026). The effect of internet involvement on digital literacy among older adults: The multiple mediations of internet use and internet sense of control. *Acta Psychologica*, 262, 106076. <https://doi.org/10.1016/j.actpsy.2025.106076>
- Hartati, S., Lutiya, L., & ... (2022). Pendidikan Kesehatan Orangtua Tentang Covid-19 Terhadap Kesehatan Mental Remaja. *Jurnal Ilmu Keperawatan* <http://www.journal.ppnijateng.org/index.php/jika/article/view/1449>
- Kuss, D. J., Louws, J., & Wiers, R. W. (2012). Online gaming addiction? Motives predict addictive play behavior in massively multiplayer online role-playing games. *Cyberpsychology, Behavior, and ...* <https://doi.org/10.1089/cyber.2012.0034>
- Lusiana, D., & Nugroho, A. B. (2024). Analisis Multi Faktor Yang Berpengaruh Terhadap Penerimaan Pada Pengguna Aplikasi Satuselat Berbasis Metode Utaut (Unified Theory Of Acceptance And Use Of Technology). *CYBERNETICS*, 8(01), 1. <https://doi.org/10.29406/cbn.v8i01.6652>

- Rahmawati, Dian; et, A. (2023). Analisis Hoaks dalam Konteks Digital: Implikasi dan Pencegahannya di Indonesia. *Innovative: Journal Of Social Science Research*, 3(2), 10819–10829. <http://j-innovative.org/index.php/Innovative/article/view/1420>
- Rahmawati, R., Permana, J., Nurdin, D., & ... (2024). Digital-Based Service In Higher Education: A Systematic Literatur Review. *Proceedings of ...*. <https://proceedings.unimal.ac.id/miceshi/article/view/515>
- Slamet, S. (2025). Smishing Guard: Strategi Pengembangan Sistem Deteksi Dan Respons Ancaman Sms Phishing. *SPIRIT: Sarana Penunjang Informasi Terkini*, 17(1), 12–23. <https://doi.org/http://dx.doi.org/10.53567/spirit.v17i1.380>
- Slamet, Soebijono, T., Erstiawan, M. S., & Churniawan, A. D. (2026). Penguatan Literasi Digital Security Awareness Bagi Anak Yatim Piatu Tingkat SD-SMA pada Yayasan Louisa. *Eskalasi: Jurnal Pengabdian Dan Pemberdayaan Masyarakat*, 1(2), 56–67.
- Soebijono, T., Erstiawan, M. S., Binawati, L., & Oktaviani, O. (2025). Kontenmu Cerminan Dirimu: Bijak di Dunia Digital Bagi Gen-Z di Lingkungan Yayasan Louisa. *Jurnal Ragam Pengabdian*, 2(2), 215–222. <https://doi.org/10.62710/tta1n864>
- Soebijono Tony, E. M. S. (2020). Peranan Revolusi Industri 4.0 terhadap Mutu Pendidikan Sekolah Menengah Kejuruan Jurusan Akuntansi. *Jurnal Bisnis Perspektif*, 12(2), 115–122.
- Sudarmo, S., Arifin, A., Pattiasina, P. J., & Wirawan, V., & Aslan (2021). The Future of Instruction Media in Indonesian Education: Systematic Review. *Al-Ishlah: Jurnal Pendidikan*, 13(2), 1302-1311. <http://journal.staihubbulwathan.id/index.php/alishlah/article/view/542>
- Surya, D., Setiawan, D., Aryani, Y. A., & Arifin, T. (2024). Cyberattacks on the accounting profession: a literatur review. *Media Riset Akuntansi, Auditing, & Informasi*, 24(2), 255-272. <https://www.e-journal.trisakti.ac.id/index.php/mraai/article/view/19953>
- Telekomunikasi, Informatika, Siber, Dan Internet - Informasi Publik, Pub. L. 95, Sekertaris Negara Republik Indonesia 1 (2018). <https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018>
- Utami, E. F., Yosep, S. P., & Erstiawan, M. S. (2026). Edukasi Nilai Sumpah Pemuda Melalui Workshop Komik Digital pada Siswa SMA. *Eskalasi: Jurnal Pengabdian Dan Pemberdayaan Masyarakat*, 1(2), 79–90.
- Wilbanks, L. R. (2021). *CyberSecurity Privacy Risks* (pp. 191–198). https://doi.org/10.1007/978-3-030-79997-7_24



- Yunus, Muh. Y., & Syukur, M. (2025). Transformasi Digital Dalam Kewirausahaan Kesehatan: Peluang Dan Tantangan Bagi Kesehatan Masyarakat. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 7639–7648. <https://doi.org/10.31004/riggs.v4i3.3164>
- Zaman, M. B., Permata Sari, I. N., Aulia, N., Tri Andari, M., Nurazizah, N. P., Yuliawati, L., Taftazani, T., Al-farisi, F. S., Nurhayati, I., Noor Sifa, R. T., Herdiansyah, D., Nugraha, A. H., Puspitasari, D., Karisma Putra, S. A., Wafa, S., Abdillah, M. W., Nurahman, F., Ruhiyat, Al Ghiffari, Moch. S., ... Hajarani, R. (2024). Penerapan Literasi Digital Desa Karyajaya Dengan pendekatan Cyber Security dan Cyber Ethic. *Jurnal PkM MIFTEK*, 5(1), 71–77. <https://doi.org/10.33364/miftek/v.5-1.1554>

