ANOA Jurnal Pengabdian Masyarakat
FAKULTAS TEKNIK UM KENDARI
E-ISSN: 2985-4660
P-ISSN: 3024-8922

Peningkatan Literasi Keamanan Siber dan Pelindungan Data Pribadi pada Remaja Desa Popalia

Ilcham [1*], Muh. Hajar Akbar [2], Jimsan [3], Muh. Dhion. R [4] , Sitti Najmia Rifai [5], Budi Wijaya Rauf [6]

[1,2,3,4] Sistem Informasi, Fakultas Teknologi Informasi, Universitas Sembilanbelas November Kolaka
[5] Komunikasi dan Penyiaran Islam, Fakultas Ushuluddin, Adab dan Dakwah, Institut Agama Islam Negeri Kendari
[6] Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Halu Oleo

**Correspondent Email: ilcham@usn.ac.id*

Article History:
Received: 30-12-2025; Received in Revised: 30-12-2025; Accepted: 31-12-2025
DOI: 10.51454/anoa.v4i02.1605

Abstrak

Akselerasi penetrasi internet di wilayah pedesaan seperti Desa Popalia menciptakan generasi remaja yang sangat adaptif terhadap teknologi digital namun memiliki manajemen risiko yang rendah. Permasalahan utama yang teridentifikasi bukan pada ketidakmampuan teknis, melainkan pada kebiasaan siber yang berisiko (risky cyber habits). Fenomena yang ditemukan adalah remaja mampu membuat kata sandi yang kompleks, namun mempraktikkan penggunaan satu kata sandi untuk berbagai platform (password reuse) dan perilaku membagikan data sensitif secara berlebihan (oversharing). Kegiatan pengabdian masyarakat ini bertujuan mengintervensi perilaku tersebut melalui pendekatan edukasi partisipatif dan simulasi teknis perlindungan akun. Metode pelaksanaan dirancang sistematis meliputi diagnosis awal, penyuluhan interaktif, simulasi audit keamanan (security checkup), dan pendampingan aktivasi fitur keamanan ganda. Melibatkan 20 remaja sebagai peserta, kegiatan ini berhasil mengubah perspektif peserta dari memandang keamanan sebagai hambatan menjadi sebuah kebutuhan primer. Hasil evaluasi menunjukkan penurunan drastis pada praktik penggunaan kata sandi tunggal dari 75% menjadi 10% dan lonjakan keberhasilan aktivasi Verifikasi Dua Langkah (2FA) mencapai 90%. Disimpulkan bahwa metode simulasi audit kebocoran data lebih efektif dalam membangun kesadaran keamanan (security awareness) dibandingkan metode ceramah normatif, serta mampu mendorong remaja melindungi privasi data mereka secara mandiri.

Kata Kunci: Desa Popalia; Literasi Keamanan Siber; Pelindungan Data Pribadi; Manajemen Kata Sandi; Remaja Digital.

Abstract

The acceleration of internet penetration in rural areas like Popalia Village has created a generation of adolescents who are adaptive to digital technology but possess low risk management skills. The primary issue identified is not technical incompetence, but rather risky cyber habits. The phenomenon discovered is that while adolescents are capable of creating complex passwords, they practice password reuse across multiple platforms and engage in oversharing sensitive data. This community service activity aims to intervene in these behaviors through a participatory education approach and technical account protection simulations. The

implementation method is designed systematically, covering initial diagnosis, interactive counseling, security audit simulations (security checkup), and assistance in activating dual security features. Involving 20 adolescents, this activity successfully shifted participants' perspectives from viewing security as an obstacle to a primary necessity. Evaluation results showed a drastic decrease in single password usage practices from 75% to 10% and a surge in the successful activation of Two-Factor Authentication (2FA) reaching 90%. It is concluded that the data breach audit simulation method is more effective in building security awareness compared to normative lecture methods, empowering adolescents to independently protect their data privacy.

Keywords: Popalia Village; Cybersecurity Literacy; Personal Data Protection; Password Management; Digital Adolescents.

1. Pendahuluan

Lanskap digital Indonesia mengalami transformasi yang sangat radikal dalam satu dekade terakhir. Pembangunan infrastruktur telekomunikasi yang masif telah membuka isolasi informasi di wilayah pedesaan, menjadikan internet sebagai kebutuhan primer yang setara dengan kebutuhan logistik lainnya. Data terbaru dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2025) mengonfirmasi bahwa penetrasi internet nasional telah menembus angka signifikan, dengan kontribusi pertumbuhan terbesar datang dari pengguna gawai (*mobile device*) di area non-urban. Dalam struktur demografi tersebut, kelompok remaja usia 13 hingga 18 tahun menempati posisi strategis sebagai "penduduk asli digital" (digital natives) yang menghabiskan sebagian besar waktu produktif mereka di ruang maya (Iskandar dkk., 2025).

Namun, statistik konektivitas yang mengesankan ini menyimpan kerentanan laten yang sering terabaikan. Di Desa Popalia, realitas di lapangan menunjukkan adanya kesenjangan yang lebar antara aksesibilitas teknologi dan literasi keamanan (*security literacy*). Remaja di desa ini sangat fasih mengoperasikan fitur-fitur hiburan di aplikasi seperti TikTok, Instagram, dan permainan daring (*mobile games*), namun mereka memiliki kesadaran yang minim terhadap manajemen risiko privasi (Fajarwati dkk., 2023).

Berdasarkan observasi awal, permasalahan di Desa Popalia bukanlah ketidaktahuan teknis atau "gaptek". Sebaliknya, remaja di desa ini cukup cerdas dalam mengeksplorasi fitur digital. Masalah utamanya adalah paradoks "Cerdas tapi Ceroboh" (*Smart but Careless*). Demi kenyamanan dan efisiensi memori, mayoritas remaja mempraktikkan penggunaan satu kata sandi untuk semua akun (*password reuse*). Mereka beranggapan bahwa mengingat banyak kata sandi adalah hal yang merepotkan. Selain itu, ditemukan pola perilaku oversharing yang mengkhawatirkan, di mana remaja dengan lugu mengunggah dokumen pribadi seperti kartu identitas atau tiket perjalanan di media sosial. Perilaku ini membuka celah lebar bagi pelaku kejahatan siber untuk melakukan rekayasa sosial (*social engineering*) dan pencurian identitas, sebuah risiko yang juga dikonfirmasi dalam studi perilaku privasi di media sosial oleh (Anjarwati, 2022; Sugeng dkk., 2022).

Secara yuridis, negara sebenarnya telah memberikan payung hukum melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Indonesia,

2022). Regulasi ini menegaskan bahwa setiap individu memiliki hak atas keamanan data pribadinya. Namun, sosialisasi mengenai UU ini sering kali berhenti di tataran elit perkotaan atau diskusi akademis, dan tidak menyentuh lapisan masyarakat desa secara substantif. Akibatnya, remaja di Desa Popalia tidak menyadari bahwa data pribadi adalah aset yang bernilai ekonomi dan hukum yang harus dilindungi (Iskandar dkk., 2025).

Kondisi ini diperburuk oleh fakta bahwa program edukasi digital yang pernah dilakukan pihak lain sebelumnya lebih berfokus pada aspek produktivitas ekonomi, seperti pemasaran digital untuk UMKM, bukan pada aspek defensif atau "kebersihan siber" (*cyber hygiene*). Oleh karena itu, kegiatan pengabdian kepada masyarakat ini hadir dengan urgensi tinggi. Tujuannya adalah membangun "tembok pertahanan pertama" di gawai remaja melalui pendekatan yang mengubah perilaku. Melalui kegiatan ini, diharapkan terbentuk norma baru bahwa menjaga privasi adalah bagian integral dari gaya hidup digital modern, bukan sekadar kewajiban teknis yang membosankan.

2.Metode

Untuk menjawab permasalahan di atas, kegiatan ini mengadopsi pendekatan Pendidikan Masyarakat Partisipatif (*Participatory Community Education*). Pendekatan ini dipilih karena karakteristik mitra sasaran (remaja) cenderung resisten terhadap metode indoktrinasi satu arah (ceramah murni), namun sangat responsif terhadap metode yang melibatkan eksperimen dan pengalaman langsung (*experiential learning*) (Hasan dkk., 2023).

2.1. Desain Kegiatan

Kerangka kerja kegiatan disusun dalam model siklus sistematis yang terdiri dari empat fase utama untuk memastikan keberhasilan transfer pengetahuan dan perubahan perilaku: a) **Fase Diagnosis (Pra-Kegiatan):** Tim pengabdi melakukan survei dan wawancara informal untuk memetakan jenis gawai, sistem operasi (Android/iOS), dan platform media sosial yang paling dominan digunakan. Fase ini juga digunakan untuk mengidentifikasi pola manajemen kata sandi yang umum diterapkan oleh remaja setempat. b) **Fase Perancangan Materi**: Menyusun kurikulum mikro yang relevan dan kontekstual. Istilah teknis yang rumit dihindari dan diganti dengan analogi sehari-hari. Materi difokuskan pada tiga pilar: Manajemen Identitas, Pencegahan Phishing, dan Pengamanan Gawai. c) **Fase Intervensi (Pelaksanaan)**: Pelaksanaan lokakarya (*workshop*) intensif bertajuk "Klinik Gawai" yang menggabungkan teori singkat dengan porsi praktik yang dominan (70% praktik, 30% teori). d) **Fase Refleksi dan Evaluasi**: Pengukuran dampak kegiatan melalui data kuantitatif dan kualitatif serta penyusunan rencana tindak lanjut bagi peserta.

2.2. Partisipan dan Lokasi

Kegiatan dipusatkan di Aula Universitas Sembilanbelas November Kolaka, lokasi yang strategis dan netral bagi seluruh warga. Mitra sasaran adalah 20 remaja terpilih dengan rentang usia 13-19 tahun. Pemilihan peserta dilakukan secara inklusif bekerja

sama dengan pengurus Karang Taruna setempat, memastikan keterwakilan dari berbagai dusun dan keseimbangan gender untuk menghindari bias gender dalam literasi teknologi (Fajarwati dkk., 2023).

2.3. Teknik Pengumpulan Data

Untuk mengukur keberhasilan kegiatan secara empiris, digunakan pendekatan metode campuran (*mixed-method*) (Miles dkk., 2014) sebagai berikut: a) **Kuantitatif**: Menggunakan instrumen Pre-test dan Post-test dengan butir soal yang mengukur dimensi pengetahuan (kognitif) dan dimensi sikap (afektif). Soal mencakup studi kasus identifikasi phishing, kekuatan kata sandi, dan pemahaman regulasi. b) **Kualitatif**: Dilakukan melalui observasi partisipatif selama sesi praktik. Fasilitator mencatat kesulitan teknis yang dihadapi peserta, respon emosional mereka saat mengetahui kerentanan akun, serta dinamika diskusi antar-peserta. c) **Studi Dokumentasi**: Menganalisis tangkapan layar (*screenshot*) bukti keberhasilan aktivasi fitur keamanan (seperti 2FA aktif) pada gawai peserta sebagai indikator keberhasilan psikomotorik.

2.4. Materi dan Instrumen Edukasi

Materi dikemas dalam modul saku digital dan cetak. Cakupan materi meliputi: (1) Anatomi serangan siber (Phishing dan Scam); (2) Manajemen kunci digital (pembuatan Passphrase); (3) Benteng lapis ganda (aktivasi Two-Factor Authentication di WhatsApp dan Instagram); dan (4) Audit jejak digital menggunakan layanan pemeriksa kebocoran data global.

3.Hasil dan Pembahasan

Kegiatan pengabdian ini menerapkan model intervensi edukasi partisipatif dengan pendekatan "*Shock Therapy*" dan pendampingan teknis intensif sebagai solusi atas rendahnya manajemen keamanan siber remaja di Desa Popalia. Fokus utama luaran kegiatan bukan sekadar pemahaman kognitif, melainkan perubahan perilaku (behavioral change) dalam mengamankan aset digital. Pelaksanaan kegiatan diawali dengan diagnosis profil digital peserta yang menyingkap fakta empiris paradoks "Cerdas tapi Ceroboh". Secara teknis, 85% peserta sangat fasih mengoperasikan gawai, namun 75% di antaranya mempraktikkan penggunaan satu kata sandi untuk semua akun (*password reuse*) demi kenyamanan. Intervensi dilakukan dengan tidak menggunakan metode ceramah konvensional, melainkan simulasi audit kebocoran data secara langsung (*live audit*).

Gambar 1. Pelaksanaan Kegiatan

Kegiatan ini melibatkan 20 remaja Desa Popalia yang berpartisipasi aktif dari tahap penyuluhan hingga praktik, sebagaimana terekam dalam dokumentasi foto pelaksanaan kegiatan pada Gambar 1. Setelah sesi pembukaan, kegiatan inti berlanjut pada pendampingan teknis "Klinik Gawai". Dalam sesi ini, solusi teknis diterapkan melalui aktivasi fitur keamanan ganda (*Two-Factor Authentication*/2FA) pada aplikasi WhatsApp dan Instagram, serta pembersihan jejak digital yang berisiko. Keberhasilan intervensi ini diukur melalui data pre-test dan post-test yang menunjukkan peningkatan signifikan, baik pada aspek kognitif maupun psikomotorik. Data capaian kegiatan disajikan secara rinci pada Tabel 1 berikut.

Tabel 1. Komparasi Indikator Kompetensi Sebelum dan Sesudah Intervensi.

No	Indikator Kompetensi	Kondisi Awal (Pre)	Kondisi Akhir (Post)	Kategori Peningkatan
1	Pemahaman Risiko *Password Reuse*	25% (Rendah)	90% (Tinggi)	Signifikan
2	Kualitas Kompleksitas Kata Sandi	80% (Baik)	95% (Sangat Baik)	Peningkatan Minor
3	Keterampilan Teknis (Aktivasi 2FA)	10% (Sangat Rendah)	90% (Sangat Tinggi)	Peningkatan Mayor
4	Kesadaran Bahaya *Oversharing*	40% (Cukup)	85% (Tinggi)	Signifikan

Berdasarkan data pada Tabel 1, temuan utama (finding) dari kegiatan ini adalah lonjakan drastis pada keterampilan teknis aktivasi 2FA yang mencapai 90%. Hal ini mengindikasikan bahwa hambatan awal peserta bukanlah ketidakmampuan teknis, melainkan kurangnya paparan informasi mengenai fitur keamanan. Secara teoritis, keberhasilan ini menunjukkan bahwa peserta bersedia melakukan tindakan perlindungan (aktivasi 2FA) karena adanya kesadaran akan keparahan dampak (*severity*) yang dibangun saat simulasi kebocoran data, serta adanya keyakinan diri (*self-efficacy*) yang tumbuh berkat pendampingan personal. Temuan ini juga memperkuat asumsi bahwa metode visual dan taktil jauh lebih efektif bagi generasi "*digital natives*" dibandingkan metode ceramah normatif. Peserta kini memandang privasi bukan sebagai upaya

menyembunyikan rahasia, melainkan sebagai hak kontrol atas data pribadi sesuai semangat regulasi pelindungan data yang berlaku.

Meskipun demikian, pelaksanaan kegiatan menghadapi tingkat kesulitan tertentu, terutama terkait infrastruktur dan kendala bahasa. Ketidakstabilan sinyal internet di lokasi sempat menghambat proses verifikasi kode OTP (*One-Time Password*), yang diatasi dengan penyediaan modem eksternal oleh tim pengabdi. Selain itu, kendala bahasa asing pada antarmuka pengaturan keamanan gawai menjadi hambatan bagi sebagian peserta, yang menuntut fasilitator untuk memandu perubahan pengaturan bahasa ke Bahasa Indonesia. Terlepas dari kendala tersebut, model pelatihan berbasis simulasi ini terbukti memiliki keunggulan adaptabilitas yang tinggi terhadap kondisi masyarakat pedesaan yang membutuhkan bukti visual nyata untuk mengubah kebiasaan lama. Peluang replikasi model ini sangat terbuka untuk diterapkan pada segmen masyarakat lain, seperti UMKM desa, guna mengamankan transaksi digital mereka.

4.Kesimpulan

Berdasarkan hasil implementasi dan evaluasi kegiatan, dapat disimpulkan bahwa permasalahan keamanan siber pada remaja di Desa Popalia bukan disebabkan oleh ketimpangan akses teknologi, melainkan oleh kebiasaan siber yang berisiko (*risky cyber habits*) seperti penggunaan kata sandi tunggal yang masif. Solusi yang diterapkan melalui metode edukasi partisipatif dan simulasi audit kebocoran data terbukti efektif menjawab permasalahan tersebut. Hal ini dibuktikan secara empiris dengan penurunan drastis praktik penggunaan kata sandi berulang dan keberhasilan 90% peserta dalam mengaktifkan sistem pertahanan ganda (2FA) pada akun media sosial mereka. Implikasi dari kegiatan ini menegaskan bahwa pendekatan literasi digital di wilayah pedesaan harus bergeser dari narasi normatif menjadi pelatihan teknis yang bersifat protektif dan aplikatif. Sebagai saran untuk keberlanjutan program, diperlukan pelibatan orang tua dalam pengawasan ekosistem digital di rumah agar praktik keamanan data yang telah diajarkan dapat menjadi budaya baru yang persisten dalam keluarga.

5.Daftar Pustaka

Anjarwati, S. (2022). *Protecting Safety and Privacy on Social Media Through Digital Literacy Competence: A Study of Library and Information Science Students UIN Sunan Kalijaga Yogyakarta*.

Fajarwati, N. K., Susilawati, E., Fitrianti, R., Handayani, P., & Zulfikar, M. (2023). Digital literacy and communication privacy in cybermedia era. *The International Journal of Politics and Sociology Research*, *11*(2), 274–279.

Hasan, M., Arisah, N., & Ahmad, M. I. S. (2023). Experiential learning model for the development of collaborative skills through Project Based Learning practicum. *JPI (Jurnal Pendidikan Indonesia)*, *12*(2), 340–349. https://doi.org/10.23887/jpiundiksha.v12i2.57376

APJII. (2025). *Laporan Survei Penetrasi dan Perilaku Pengguna Internet Indonesia Tahun 2025*. APJII. https://survei.apjii.or.id/survei

Iskandar, R., Maksum, A., & Marini, A. (2025). Digital citizenship literacy in Indonesia: The role of privacy awareness and social campaigns. *Social Sciences & Humanities Open*, *12*, 101697. https://doi.org/10.56873/jpkm.v5i2.2670

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook*. SAGE Publications.

Sugeng, S., Fitria, A., & Rohman, A. N. R. A. N. (2022). Promoting digital literacy for the prevention of risk behavior in social media for adolescents. *Jurnal Keamanan Nasional*, *8*(1). https://doi.org/10.31599/7cv3sj91

Indonesia, H. R. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.