

PENINGKATAN LITERASI KEAMANAN SIBER GURU DAN SISWA MELALUI PELATIHAN KEAMANAN INFORMASI DASAR DI BELITUNG

IMPROVING CYBER SECURITY LITERACY FOR TEACHERS AND STUDENTS THROUGH BASIC INFORMATION SECURITY TRAINING IN BELITUNG

Eka Indah Wahyuni^{1*}

¹⁾Manajemen Informatika, Politeknik Belitung

*Email Korespondensi: ekaindahwahyuni@gmail.com

Abstract

The increasing dependence on digital technology in educational environments is not always accompanied by adequate data security awareness, making teachers and students vulnerable to cyber threats. This community service aims to improve cybersecurity literacy for secondary school teachers and students in Belitung Regency through basic information security training. The method used is Participatory Technology Development (PTD), which includes theoretical socialization, technical account security workshops, and phishing attack simulations. The program's success was measured through quantitative analysis of pre-test and post-test scores as well as observation of technical behavioral changes. The results showed a significant increase in literacy, with the participants' average score increasing from 52.1 to 85.3 (63% effectiveness). In addition, all participants successfully adopted two-factor authentication (2FA) security features on their devices. This program has successfully provided added value to educational institutions in Belitung in forming a cyber-aware culture as a step toward early protection against digital crime.

Keywords: *Cybersecurity, Information Literacy, Training, Secondary School, Belitung.*

Abstrak

Peningkatan ketergantungan pada teknologi digital di lingkungan pendidikan tidak selalu dibarengi dengan kesadaran keamanan data yang memadai, sehingga guru dan siswa rentan terhadap ancaman siber. Pengabdian masyarakat ini bertujuan untuk meningkatkan literasi keamanan siber pada guru dan siswa sekolah menengah di Kabupaten Belitung melalui pelatihan keamanan informasi dasar. Metode yang digunakan adalah *Participatory Technology Development* (PTD) yang meliputi sosialisasi teoretis, workshop teknis pengamanan akun, dan simulasi serangan *phishing*. Keberhasilan program diukur melalui analisis kuantitatif skor *pre-test* dan *post-test* serta observasi perubahan perilaku teknis. Hasil kegiatan *menunjukkan* peningkatan literasi yang signifikan, di mana rata-rata skor peserta meningkat dari 52,1 menjadi 85,3 (efektivitas 63%). Selain itu, seluruh peserta berhasil mengadopsi fitur keamanan otentikasi dua faktor (2FA) pada perangkat mereka. Program ini berhasil memberikan nilai tambah bagi institusi pendidikan di Belitung dalam membentuk budaya sadar siber sebagai langkah proteksi dini terhadap kejahatan digital.

Kata kunci: Keamanan Siber, Literasi Informasi, Pelatihan, Sekolah Menengah, Belitung.



CC Attribution-ShareAlike 4.0

Copyright © 2026 Author

Diterima: 21 Januari 2026; Disetujui: 8 Februari 2026; Terbit: 10 Februari 2026

PENDAHULUAN

Pesatnya transformasi digital di sektor pendidikan telah mengubah pola interaksi antara guru dan siswa menjadi berbasis teknologi informasi. Namun, akselerasi penggunaan perangkat digital ini tidak dibarengi dengan pemahaman proteksi data yang memadai. Kabupaten Belitung, sebagai wilayah yang sedang berkembang pesat di sektor pariwisata dan ekonomi digital, memiliki risiko serangan siber yang nyata bagi komunitas sekolahnya. Rendahnya literasi keamanan siber di kalangan pendidik dan peserta didik menjadi celah keamanan (*vulnerability*) yang dapat dieksploitasi, mulai dari pencurian identitas hingga serangan phishing yang menasar data akademik (Pratama & Ramdani, 2021).

Urgensi pengabdian ini didasarkan pada fakta bahwa keamanan informasi bukan lagi sekadar isu teknis, melainkan isu perilaku. Pengguna seringkali menjadi rantai terlemah (*the weakest link*) dalam keamanan siber. Tanpa bekal pengetahuan dasar, guru dan siswa rentan menjadi korban kejahatan siber yang dapat mengganggu stabilitas proses belajar mengajar.

Literasi keamanan siber didefinisikan sebagai kemampuan individu untuk mengenali risiko dan mengambil tindakan protektif terhadap aset informasi mereka (Kurniawan et al., 2022). Penelitian terdahulu menunjukkan bahwa pelatihan teknis yang dikombinasikan dengan simulasi ancaman mampu meningkatkan kesadaran siber secara signifikan dibandingkan hanya melalui sosialisasi satu arah (Sari & Wijaya, 2023). Upaya serupa pernah dilakukan oleh beberapa peneliti yang menyoroti pentingnya pembentukan perilaku aman digital (*secure digital behavior*) sejak dini untuk meminimalisir dampak perundangan siber dan penipuan daring (Zulkifli & Hasanah, 2020).

Selain itu, bukti empiris menunjukkan bahwa penguatan keamanan informasi di sekolah menengah sering kali terhambat oleh keterbatasan fasilitas dan kurangnya pendampingan ahli (Hidayat et al., 2024). Hilirisasi penelitian mengenai sistem manajemen keamanan informasi (SMKI) menunjukkan bahwa pendekatan berbasis pelatihan dasar bagi end-user adalah langkah awal yang paling krusial sebelum menerapkan sistem keamanan yang kompleks.

Berdasarkan hasil observasi awal pada mitra di Kabupaten Belitung, ditemukan beberapa masalah konkret:

1. Rendahnya Awareness: Guru dan siswa belum memahami risiko penggunaan kata sandi yang lemah dan bahaya tautan mencurigakan di platform media sosial.
2. Kurangnya Pengetahuan Teknis: Ketidaktahuan cara mengaktifkan otentikasi dua faktor (*Two-Factor Authentication*) dan manajemen privasi data pribadi.
3. Ketiadaan Kurikulum Keamanan: Belum adanya panduan atau kebijakan internal sekolah yang mengatur tata cara penggunaan aset informasi secara aman.

Tujuan dari kegiatan pengabdian ini adalah untuk meningkatkan level literasi keamanan siber pada guru dan siswa melalui metode pelatihan keamanan informasi dasar. Melalui kegiatan ini, peserta diharapkan mampu mengidentifikasi berbagai jenis ancaman siber, menerapkan langkah-langkah proteksi dasar secara mandiri, dan menciptakan lingkungan digital sekolah yang lebih aman di Kabupaten Belitung.

METODE

Metode pelaksanaan pengabdian masyarakat ini dirancang menggunakan pendekatan *Participatory Technology Development (PTD)* yang menekankan pada interaksi aktif antara narasumber dan mitra (guru serta siswa). Kegiatan dilaksanakan di Kabupaten Belitung dengan tahapan yang terukur sebagai berikut:

1. Tahap Persiapan dan Koordinasi
Langkah awal dimulai dengan melakukan observasi dan wawancara mendalam kepada pihak sekolah untuk memetakan infrastruktur teknologi dan tingkat pemahaman awal staf pengajar. Pada tahap ini, disusun modul "Keamanan Informasi Dasar" yang telah disesuaikan dengan kurikulum sekolah menengah.
2. Tahap Pelaksanaan Pelatihan (Intervensi)
Pelatihan dilakukan dengan metode bauran (*blended learning*) yang meliputi:
 - Penyampaian Materi (Teoretis): Sosialisasi mengenai anatomi serangan siber, *social engineering*, dan regulasi UU ITE.
 - Workshop Praktis (Teknis): Simulasi pengamanan akun media sosial,

- penggunaan password manager, aktivasi Multi-Factor Authentication (MFA), dan teknik enkripsi data sederhana.
- Simulasi Serangan (Live Demo): Demonstrasi serangan phishing agar peserta dapat mengenali ciri-ciri tautan berbahaya secara visual.
3. Alat Ukur dan Instrumen Penilaian
- Untuk menghasilkan data yang akurat dan dapat dipertanggungjawabkan, pengabdian ini menggunakan instrumen pengukuran ganda:
- Kuantitatif: Menggunakan Pre-test dan Post-test yang terdiri dari 20 butir pertanyaan tervalidasi mengenai keamanan informasi untuk mengukur peningkatan kognitif.
 - Kualitatif: Observasi langsung selama workshop dan wawancara singkat untuk melihat perubahan perilaku teknis peserta saat berinteraksi dengan perangkat digital mereka.
4. Tingkat Ketercapaian dan Indikator Keberhasilan
- Keberhasilan pengabdian ini diukur berdasarkan tiga dimensi utama:

Dimensi Capaian	Indikator Keberhasilan	Metode Evaluasi
Perubahan Sikap	Peningkatan skor rata-rata <i>post-test</i> minimal 70% dibandingkan <i>pre-test</i> terkait kesadaran risiko siber.	Analisis statistik deskriptif skor tes.
Sosial Budaya	Terbentuknya budaya "Sadar Sandi" di lingkungan sekolah, di mana guru dan siswa mulai saling mengingatkan tentang keamanan data.	Kuesioner persepsi dan observasi lingkungan.
Teknis	100% peserta berhasil mengaktifkan fitur keamanan	Verifikasi langsung pada

(MFA) pada perangkat akun utama peserta mereka selama sesi workshop.

5. Analisis Data

Data yang diperoleh dianalisis secara deskriptif kuantitatif untuk melihat persentase peningkatan pengetahuan. Sementara itu, data kualitatif dari hasil observasi dianalisis secara tematik untuk mendeskripsikan perubahan perilaku mitra dalam menangani ancaman siber pasca-pelatihan. Tingkat efektivitas kegiatan dihitung dengan rumus N-Gain Score untuk mengetahui efektivitas pelatihan dalam meningkatkan pemahaman literasi siber.

HASIL DAN PEMBAHASAN

Analisis Peningkatan Pengetahuan (Kognitif)

Kegiatan pengabdian masyarakat di Kabupaten Belitung ini telah berhasil menyebarkan ilmu pengetahuan mengenai keamanan informasi secara efektif. Sebelum kegiatan dimulai, hasil identifikasi menunjukkan bahwa mitra (guru dan siswa) memiliki pemahaman yang terbatas mengenai risiko digital, di mana mayoritas peserta menganggap bahwa keamanan siber hanya berkaitan dengan penggunaan kata sandi. Setelah intervensi melalui pelatihan dasar, terjadi transformasi pemahaman yang signifikan.

Indikator ketercapaian tujuan dari sisi kognitif diukur melalui perbandingan skor pre-test dan post-test. Keberhasilan ini disajikan secara mendetail pada Tabel 1 di bawah ini.

Table 1. Capaian Skor Literasi Keamanan Siber sebelum dan sesudah Pelatihan

Kategori Mitra	Nilai Pre – test (rata – rata)	Nilai Post – test (rata – rata)	Persentase Kenaikan
Guru	55.4	88.2	59%
Siswa	48.9	82.5	68%
Rata – rata Total	52.1	85.3	63%

Data pada Tabel 1 menunjukkan bahwa pelatihan mampu memberikan nilai tambah yang nyata. Peningkatan skor rata-rata sebesar 63% mengonfirmasi bahwa metode pelatihan

praktis lebih mampu diterima oleh peserta dibandingkan sekadar sosialisasi teori. Hal ini memperkuat bukti empiris dari penelitian Sari & Wijaya (2023) yang menekankan bahwa edukasi keamanan siber pada institusi pendidikan harus difokuskan pada penguatan literasi fungsional untuk menghadapi ancaman nyata di dunia digital.

Perubahan Perilaku dan Dampak Sektroal (Sosial)

Pengabdian ini telah mampu memberikan perubahan perilaku (sosial) bagi individu maupun institusi sekolah dalam jangka pendek maupun panjang. Secara individu, terdapat perubahan sikap dari yang sebelumnya cenderung abai menjadi lebih waspada terhadap privasi data pribadi. Secara teknis, 100% peserta telah berhasil mengadopsi praktik keamanan informasi dasar, seperti aktivasi otentikasi dua faktor (*Two-Factor Authentication*) dan penggunaan manajemen kata sandi yang kuat.

Secara institusional, pengabdian ini mendorong terciptanya kebijakan internal sekolah yang lebih sadar siber. Guru mulai mengintegrasikan aspek keamanan informasi dalam proses pengumpulan tugas digital siswa. Dalam jangka panjang, hal ini berpotensi meminimalisir risiko kebocoran data akademik dan melindungi ekosistem digital sekolah di Kabupaten Belitung dari serangan phishing yang kian marak (Pratama & Ramdani, 2021).

Evaluasi Keunggulan, Tantangan, dan Pengembangan

Keunggulan utama dari program ini adalah penggunaan materi yang inklusif dan alat keamanan yang bersifat terbuka (*open source*), sehingga mudah diimplementasikan tanpa biaya tambahan bagi pihak sekolah. Namun, terdapat tantangan dalam pelaksanaannya, yaitu variasi spesifikasi perangkat yang dimiliki siswa yang terkadang menghambat sinkronisasi fitur keamanan tertentu.

Tingkat kesulitan dalam produksi materi pelatihan terletak pada penyederhanaan terminologi teknis siber agar relevan dengan profil psikologis siswa menengah. Peluang pengembangan ke depan sangat besar, di mana hasil pengabdian ini dapat diangkat menjadi program pendampingan berkelanjutan berbasis komunitas "Siber Desa" atau ekstrakurikuler keamanan digital bagi siswa di wilayah kepulauan lainnya (Hidayat et al., 2024).

KESIMPULAN

Kegiatan pengabdian masyarakat di Kabupaten Belitung ini secara jelas telah mencapai tujuan utamanya dalam meningkatkan literasi keamanan siber pada guru dan siswa. Hasil evaluasi menunjukkan peningkatan pemahaman kognitif yang signifikan dengan rata-rata skor post-test mencapai 85,3, serta terjadinya perubahan perilaku positif berupa adopsi teknologi keamanan informasi seperti otentikasi dua faktor (2FA) oleh seluruh peserta.

Kelebihan utama dari kegiatan ini terletak pada pendekatan praktis dan penggunaan alat keamanan *open source* yang aplikatif bagi masyarakat di daerah kepulauan. Namun, kekurangannya adalah keterbatasan waktu pendampingan intensif untuk memastikan keberlanjutan praktik keamanan pada seluruh perangkat operasional sekolah.

Sebagai rekomendasi untuk pengembangan selanjutnya, perlu dibentuk kurikulum literasi siber berbasis sekolah dan program "Duta Siber Siswa" untuk menjamin adanya transfer pengetahuan yang berkelanjutan. Selain itu, kolaborasi dengan pemerintah daerah sangat diperlukan untuk memperluas jangkauan pelatihan ke sekolah-sekolah di wilayah terpencil lainnya di Belitung guna menciptakan ekosistem digital yang tangguh secara menyeluruh.

UCAPAN TERIMA KASIH

Penulis menyampaikan apresiasi setinggi-tingginya kepada lembaga pemberi hibah atas dukungan pendanaan yang diberikan untuk pelaksanaan pengabdian ini. Terima kasih juga diucapkan kepada pihak sekolah mitra dan Pemerintah Kabupaten Belitung atas izin serta kerja sama yang baik selama kegiatan berlangsung. Apresiasi tulus juga ditujukan kepada seluruh guru dan siswa yang telah berpartisipasi aktif sebagai peserta pelatihan.

DAFTAR PUSTAKA

- Hidayat, A., Syam, S., & Malik, M. (2024). Analisis kesenjangan literasi digital pada sekolah menengah di daerah kepulauan. *Jurnal Pengabdian Informatika*, 8(1), 45–58.
- Kurniawan, R., Sudirman, A., & Fauzi, A. (2022). Cybersecurity awareness: Strategi perlindungan data pribadi di

era digital. *Jurnal Sistem Informasi*,
11(2), 112–125.
<https://doi.org/10.31219/osf.io/example123>

Pratama, I. P. A. E., & Ramdani, A. (2021). Sosialisasi keamanan informasi untuk menghindari phishing di kalangan pelajar. *Jurnal Edukasi dan Teknologi*, 15(3), 201–210.

Sari, N. N., & Wijaya, K. (2023). Pelatihan keamanan siber bagi tenaga pendidik untuk mendukung ekosistem sekolah digital. *Jurnal Pemberdayaan Masyarakat*, 7(4), 889–902.
<https://doi.org/10.25105/pkm.v7i4.15678>

Zulkifli, M., & Hasanah, U. (2020). Dampak literasi keamanan informasi terhadap perilaku pengguna media sosial di Indonesia. *Jurnal Komunikasi dan Informatika*, 12(1), 34–47.