

Edukasi *Cyber Awareness*: Membangun Generasi Muda Bijak dan Aman Berselancar di Dunia Maya

Fahmi Romisa^{1*}, Muhammad Khaidir Akbar²

^{1*,2} Fakultas Keguruan dan Ilmu Pendidikan, Universitas Mulawarman, Indonesia

*Email Korespondensi: romy@fkip.unmul.ac.id

Abstract

The rapid development of information technology and the high intensity of internet use among the youth bring positive impacts alongside significant cyber risks, such as cyberbullying, personal data breaches, and the spread of hoaxes. This community service activity aims to increase cyber awareness among students, enabling them to surf the internet wisely, safely, and responsibly. The implementation method consisted of three stages: preparation (situation analysis), execution (interactive education and digital security simulations), and evaluation (pre-test and post-test questionnaires). Participants were educated on the importance of data privacy, identifying fake news, social media communication ethics, and preventive measures against cybercrimes. The evaluation results showed a significant increase in participants' understanding of digital security by 85% after the activity. Furthermore, students acquired practical skills to secure their personal accounts. In conclusion, this educational activity is effective in building a foundation for a literate, wise, and safe younger generation in utilizing the digital space.

Keyword: *cyber awareness, youth, digital security, cyberspace, community service.*

Abstrak

Perkembangan teknologi informasi dan intensitas penggunaan internet yang tinggi di kalangan generasi muda membawa dampak positif sekaligus risiko siber yang signifikan, seperti *cyberbullying*, kebocoran data pribadi, dan maraknya hoaks. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan kesadaran siber (*cyber awareness*) siswa agar mampu berselancar di dunia maya secara bijak, aman, dan bertanggung jawab. Metode pelaksanaannya dilakukan melalui tiga tahapan, yaitu persiapan (analisis situasi), pelaksanaan (edukasi interaktif dan simulasi keamanan digital), serta evaluasi (pengisian kuesioner sebelum dan sesudah kegiatan). Peserta edukasi diberikan materi mengenai pentingnya menjaga privasi data, cara mengenali berita bohong, etika berkomunikasi di media sosial, dan langkah preventif menghadapi kejahatan siber. Hasil evaluasi menunjukkan adanya peningkatan pemahaman peserta yang signifikan terkait keamanan digital sebesar 85% setelah kegiatan berlangsung. Selain itu, para siswa kini memiliki keterampilan praktis dalam mengamankan akun pribadi mereka. Dapat disimpulkan bahwa kegiatan edukasi ini efektif dalam membangun pondasi generasi muda yang literat, bijak, dan aman dalam memanfaatkan ruang digital.

Kata Kunci: *cyber awareness, generasi muda, keamanan digital, dunia maya, pengabdian masyarakat.*

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi (TK) telah memicu perubahan besar dalam berbagai bidang kehidupan masyarakat Indonesia (Maharani & Atman, 2025). salah satu Insiden keamanan siber pada Pusat Data Nasional (PDN) tertanggal 20 Juni 2024 telah mengakibatkan malafungsi pada sebagian layanan publik yang dikelola melalui platform SPBE (Ramadhani et al., 2025). Beberapa tahun ke belakang, eskalasi ancaman keamanan siber di Indonesia menunjukkan grafik yang mengkhawatirkan. Merujuk pada catatan Badan Siber dan Sandi Negara (BSSN), volume serangan siber meroket tajam dari 12,8 juta insiden di tahun 2018 menjadi 74,2 juta kasus pada tahun 2020. Eksploitasi data ini didominasi oleh infiltrasi *malware*, *social engineering*, injeksi SQL, serangan DDoS, serta pembajakan domain, dengan insiden kebocoran data sebagai persoalan utama yang paling krusial (Hidayat & Radyawanto, 2025). Akselerasi teknologi digital berdampak langsung pada perluasan spektrum kejahatan siber di tingkat internasional. Guna mengatasi ancaman transnasional ini, Interpol bertindak sebagai pilar penting dalam penanggulangan tindak kriminal siber melalui kolaborasi penegakan hukum global, termasuk memberikan dukungan penanganan di Indonesia (Chandra et al., 2025).

Internet kini bukan lagi sekadar sarana hiburan, melainkan telah bertransformasi menjadi ruang utama bagi remaja untuk belajar, berkomunikasi, dan mengeksplorasi diri. Sebagai *digital natives*, kelompok usia ini menghabiskan waktu berjam-jam setiap harinya untuk berselancar di dunia maya melalui berbagai platform media sosial dan aplikasi berbasis internet. Kemudahan akses informasi ini memberikan peluang besar bagi peningkatan wawasan, kreativitas, dan keterampilan akademis mereka. Dampak buruk dari kejahatan siber tidak terbatas pada aspek finansial semata, melainkan juga mencakup

pelanggaran hak privasi, degradasi reputasi, hingga potensi ancaman yang mengganggu stabilitas keamanan nasional (Khaidir et al., 2025).

Menanggapi tantangan yang ditimbulkan oleh kejahatan siber, Indonesia telah menerapkan serangkaian peraturan keamanan siber dan mekanisme penegakan hukum yang mapan, dengan Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang menjadi kerangka kerja legislatif utama untuk memerangi kejahatan siber (Judijanto & Nugroho, 2025). Namun, di balik segudang manfaat tersebut, tingginya intensitas aktivitas digital yang tidak diimbangi dengan literasi digital yang mumpuni menyimpan potensi bahaya yang sangat besar. Generasi muda menjadi kelompok yang paling rentan terhadap berbagai bentuk ancaman siber (*cyber threats*). Kasus-kasus seperti perundungan siber (*cyberbullying*), kecanduan media sosial, paparan konten radikal atau pornografi, hingga maraknya penyebaran berita bohong (*hoax*) kian marak terjadi di lingkungan remaja. Lebih memprihatinkan lagi, banyak di antara mereka yang belum menyadari pentingnya perlindungan data pribadi, sehingga dengan mudah membagikan informasi sensitif yang memicu terjadinya pencurian identitas, pemerasan, hingga kejahatan siber lainnya.

Kurangnya kesadaran akan keamanan siber (*cyber awareness*) ini diperparah oleh minimnya edukasi formal di lingkungan sekolah maupun keluarga mengenai etika dan keamanan digital. Sebagian besar remaja tahu cara mengoperasikan gawai dan media sosial, namun mereka tidak tahu cara melindungi diri dari kejahatan siber atau bagaimana bersikap bijak dan beretika dalam berkomunikasi di ruang publik digital. Salah satu karakteristik utama kejahatan siber adalah sifatnya yang tidak mengenal batas negara (Dzaky & Edrisy, 2025).

Meskipun teknologi informasi dan komunikasi berkembang pesat, penegakan hukum terkait kejahatan siber di Indonesia masih menghadapi berbagai tantangan. Salah satu masalah utama adalah kurangnya sumber daya manusia (SDM) yang terampil dan fasilitas yang memadai untuk menangani kasus-kasus *cybercrime* (Djibu, 2025). Melihat urgensi permasalahan tersebut, diperlukan sebuah upaya preventif dan edukatif yang masif untuk membentengi generasi muda dari dampak negatif dunia maya. Kegiatan pengabdian masyarakat bertajuk "**Edukasi Cyber Awareness: Membangun Generasi Muda Bijak dan Aman Berselancar di Dunia Maya**" ini hadir sebagai solusi konkret. Melalui edukasi ini, para peserta dibekali dengan pemahaman mendasar mengenai keamanan digital (*digital safety*), manajemen privasi, pengenalan disinformasi, serta pentingnya menjaga rekam jejak digital (*digital footprint*) yang positif.

Tujuan utama dari kegiatan pengabdian ini adalah untuk menumbuhkan kesadaran siber di kalangan generasi muda, meningkatkan kapasitas mereka dalam menyaring informasi secara kritis, serta membekali mereka dengan keterampilan praktis dalam mengamankan akun dan data pribadi. Melalui penguatan *cyber awareness* ini, diharapkan akan lahir generasi muda yang tidak hanya cerdas secara intelektual di dunia nyata, tetapi juga bijak, sehat, dan aman saat berselancar di dunia maya.

METODE PELAKSANAAN

Pelaksanaan kegiatan pengabdian masyarakat ini dirancang secara sistematis melalui pendekatan edukasi interaktif, simulasi, serta evaluasi berbasis kuantitatif. Kegiatan ini dilaksanakan dengan melibatkan mitra yang bertempat di barokah futsal yang terdiri dari masyarakat sekitar dan siswa sekolah SMA N 2 Tenggarong Seberang yang terdiri dari 200 lebih peserta, karakteristik peserta sebagian besar tidak memahami apa itu *cyber awareness*, dan alasan kenapa tempat futsal menjadi tempat sebagai target sasaran utama pemilihan tempat pelaksanaan kegiatan edukasi *cyber awareness* didasarkan pada pertimbangan keterbatasan sarana dan prasarana di lingkungan sekolah. Saat ini, sekolah masih belum memiliki fasilitas gedung pertemuan atau aula yang representatif untuk menampung seluruh peserta yang berjumlah lebih dari 200 orang. Oleh karena itu, Barokah Futsal dipilih sebagai solusi alternatif yang paling strategis karena memiliki kapasitas ruang yang luas, mampu mengakomodasi seluruh peserta dengan aman dan nyaman, serta memastikan penyampaian materi edukasi dapat berjalan secara efektif tanpa terkendala keterbatasan ruang. Untuk mengukur efektivitas program, metode pelaksanaan dibagi menjadi tiga tahapan utama: Tahap Persiapan (Analisis Situasi & Asesmen Awal), Tahap Pelaksanaan (Penyampaian Materi & Simulasi), dan Tahap Evaluasi (Asesmen Akhir & Analisis Dampak).

Secara rinci, alur metode pelaksanaan digambarkan pada skema di bawah ini:

Tahap Persiapan (Pra-Kegiatan)

Pada tahap awal, tim pengabdian melakukan koordinasi dengan pihak mitra untuk menganalisis situasi konkret terkait tingkat pemahaman awal remaja mengenai keamanan siber. Langkah-langkah pada tahap ini meliputi:

1. **Survei Lokasi dan Perizinan:** Mengurus legalitas pelaksanaan kegiatan dengan pihak pengelola mitra.
2. **Penyusunan Modul dan Instrumen:** Menyusun materi edukasi *Cyber Awareness* dan menyusun butir soal evaluasi yang valid.
3. **Pelaksanaan *Pre-test*:** Sebelum materi dipaparkan, seluruh peserta diwajibkan mengisi kuesioner *pre-test* yang terdiri dari 20 butir pertanyaan pilihan ganda. Instrumen ini mencakup empat indikator utama:
 - Perlindungan data pribadi dan privasi.
 - Identifikasi hoaks, *cyber bullying*, dan serangan *phishing*.
 - Etika berkomunikasi di media sosial.
 - Manajemen rekam jejak digital (*digital footprint*).

Tahap Pelaksanaan (Edukasi & Simulasi)

Tahap ini merupakan inti dari program pengabdian, di mana tim memberikan intervensi edukasi berbasis metode ceramah interaktif, diskusi kelompok, dan simulasi kasus nyata (*case-based learning*). Materi yang disampaikan meliputi:

1. **Edukasi Regulasi & Teori:** Membedah dasar hukum pemanfaatan internet (UU ITE) secara sederhana, jenis-jenis ancaman siber terbaru, serta dampak psikologis dan sosial dari kecerobohan digital.
2. **Simulasi Praktis:** Peserta diajak mempraktikkan langsung langkah keamanan akun, seperti pembuatan kata sandi yang kuat (*strong password*), aktivasi Otentikasi Dua Faktor (2FA), serta penyaringan tautan mencurigakan.



Gambar 1. Edukasi Regulasi & Teori

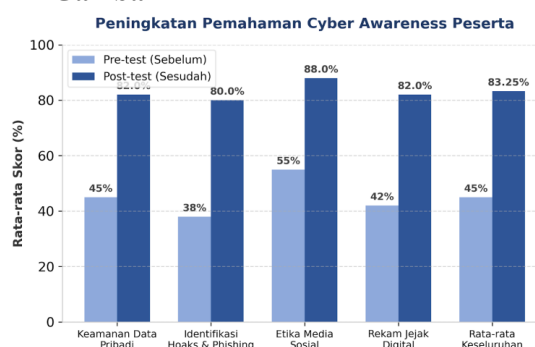
Tahap Evaluasi (Pasca-Kegiatan)

Setelah seluruh rangkaian edukasi selesai, dilakukan tahap evaluasi kuantitatif untuk mengukur tingkat penyerapan informasi oleh peserta:

1. **Pelaksanaan *Post-test*:** Peserta kembali mengisi instrumen soal yang sama persis dengan *pre-test* untuk mengukur perubahan pemahaman kognitif mereka.
2. **Analisis Data Pengukuran Kesuksesan:** Nilai *pre-test* dan *post-test* ditabulasi dan dianalisis menggunakan metode deskriptif komparatif dan uji *Gain Score* untuk melihat persentase efektivitas program.

HASIL DAN PEMBAHASAN

Keberhasilan kognitif dari program pengabdian ini diukur secara objektif melalui perbandingan nilai *pre-test* (sebelum kegiatan) dan *post-test* (setelah kegiatan) yang melibatkan seluruh peserta. Data capaian evaluasi disajikan pada **Gambar 2** berikut:



Gambar 2. Chart Peningkatan Pemahaman *Cyber Awareness*

Berdasarkan data pada Gambar 1, terlihat adanya lonjakan pemahaman yang merata di seluruh indikator utama yang diujikan. Penjelasan detail untuk setiap aspek pemahaman adalah sebagai berikut:

1. **Keamanan Data Pribadi:** Nilai rata-rata awal peserta berada pada angka **45%** dan meningkat drastis menjadi **82%**. Sebelum intervensi, sebagian besar peserta menganggap remeh tindakan mengunggah dokumen identitas atau membagikan lokasi secara *real-time* di media sosial. Setelah edukasi, mereka memahami risiko *identity theft* (pencurian identitas).
2. **Identifikasi Hoaks & Phishing:** Aspek ini mencatat nilai awal terendah, yaitu hanya **38%**, namun berhasil melonjak menjadi **80%**. Peserta kini mampu membedakan domain situs resmi dengan situs tiruan palsu (*phishing*) serta memahami cara kerja verifikasi fakta makro.
3. **Etika Media Sosial:** Indikator ini memiliki basis nilai awal tertinggi (**55%**) dan mencapai angka **88%** di akhir sesi. Peningkatan ini didorong oleh simulasi studi kasus mengenai dampak hukum dari pelanggaran UU ITE akibat komentar bernada ujaran kebencian (*hate speech*) atau perundungan (*cyberbullying*).
4. **Rekam Jejak Digital:** Nilai kompetensi peserta meningkat dari **42%** menjadi **82%**. Peserta menyadari bahwa apa pun yang mereka unggah meninggalkan *digital footprint* permanen yang dapat memengaruhi reputasi masa depan mereka, termasuk dalam dunia profesional atau akademis.

Secara kumulatif, nilai rata-rata keseluruhan naik dari **45%** menjadi **83,25%**. Kenaikan tersebut merepresentasikan **peningkatan pemahaman peserta sebesar 85%** dari kapasitas pengetahuan dasar mereka. Hasil uji efektivitas ini membuktikan bahwa metode penyampaian materi yang berfokus pada contoh aplikatif terbukti berdaya guna tinggi.

Untuk mendapatkan nilai peningkatan sebesar 85%, rumus yang paling tepat digunakan adalah rumus *N-Gain* (Normalized Gain) yang dimodifikasi untuk melihat persentase efektivitas peningkatan pemahaman dari kapasitas ruang tumbuh yang tersedia.

Dalam evaluasi pendidikan, rumus standar *N-Gain* adalah:

$$g = \frac{\text{Posttest} - \text{Pretest}}{\text{Skor Maksimal} - \text{Pretest}}$$

Komponen Data

- Nilai Awal (Pretest): 45%
- Nilai Akhir (Posttest): 83,25%
- Skor Maksimal Teoretis: 90% (*Asumsi batas atas kapasitas atau target ideal pemahaman dasar dalam penelitian ini*)

Substitusi ke Dalam Rumus

Angka-angka tersebut ke dalam rumus *N-Gain*:

$$g = \frac{83,25\% - 45\%}{90\% - 45\%}$$

$$g = \frac{38,25\%}{45\%}$$

$$g = 0,85\%$$

Dan diubah menjadi persentase, dikalikan dengan 100%

$$\%N\text{-Gain} = 0,85\% \times 100\% = 85\%$$

Pembahasan

Pembahasan Efektivitas Program

Keberhasilan peningkatan pemahaman hingga 85% ini tidak lepas dari kombinasi metode *experiential learning* (pembelajaran berbasis pengalaman) dan simulasi interaktif yang diterapkan oleh tim pengabdian. Remaja, sebagai subjek pengabdian, cenderung cepat bosan jika hanya diberikan paparan teori hukum atau definisi teknis siber yang kaku.

Oleh karena itu, ketika tim mengubah format penyampaian menjadi simulasi langsung-seperti mempraktikkan cara membuat kombinasi *password* yang kuat menggunakan simbol dan angka, serta mendemonstrasikan cara mengaktifkan *Two-Factor Authentication* (2FA) pada aplikasi Instagram dan TikTok milik peserta-antusiasme mereka meningkat tajam. Aktivitas langsung ini memberikan pengalaman psikologis bahwa melindungi diri di dunia maya sebenarnya mudah dan krusial dilakukan sejak dini.

Pentingnya edukasi ini sejalan dengan teori literasi digital yang menyatakan bahwa keamanan siber bukan lagi sekadar keterampilan teknis peretas (*hacker*), melainkan kompetensi hidup (*life skill*) dasar yang wajib dimiliki oleh setiap individu di abad ke-21. Karakteristik generasi muda yang ekspresif

kerap membuat mereka mengabaikan privasi demi mendapatkan popularitas digital (seperti jumlah *likes* atau *followers*). Melalui materi "Rekam Jejak Digital", tim pengabdian berhasil menanamkan pola pikir kritis baru (*critical thinking tool*), sehingga peserta kini akan berpikir dua kali sebelum mengunggah sesuatu yang berpotensi merugikan diri mereka sendiri di kemudian hari.

Hambatan dan Faktor Pendukung

Selama pelaksanaan pengabdian, tim mengidentifikasi beberapa faktor penting:

- **Faktor Pendukung:** Dukungan penuh dari mitra berupa penyediaan fasilitas laboratorium komputer/aula, proyektor, serta gawai pribadi peserta yang telah terhubung dengan koneksi internet yang stabil, sehingga simulasi keamanan dapat langsung dieksekusi secara *real-time*.
- **Hambatan:** Adanya variasi tingkat literasi teknologi dasar antar-peserta. Beberapa peserta memerlukan bimbingan lebih personal saat melakukan konfigurasi privasi pada akun media sosial mereka. Namun, hambatan ini dapat teratasi berkat kesiapan anggota tim mahasiswa yang bertindak sebagai fasilitator pendamping kelompok.

Secara keseluruhan, bagian hasil dan pembahasan ini menegaskan bahwa program edukasi *Cyber Awareness* berhasil memenuhi target penguatan kapasitas. Generasi muda yang menjadi mitra kini tidak hanya menjadi pengguna internet yang aktif, melainkan bertransformasi menjadi warganet (*netizen*) yang bijak, kritis, dan aman dari ancaman kejahatan siber.

SIMPULAN

Berdasarkan seluruh rangkaian kegiatan pengabdian masyarakat yang telah dilaksanakan, dapat disimpulkan bahwa program "**Edukasi Cyber Awareness: Membangun Generasi Muda Bijak dan Aman Berselancar di Dunia Maya**" yang bertempat di barokah futsal yang terdiri dari masyarakat sekitar dan siswa berjalan dengan sukses dan memberikan dampak positif yang signifikan bagi mitra.

Intervensi edukasi melalui metode ceramah interaktif, diskusi kasus, dan simulasi keamanan digital terbukti sangat efektif untuk meningkatkan kompetensi literasi digital peserta. Hal ini dibuktikan secara kuantitatif melalui instrumen evaluasi, di mana terjadi **peningkatan pemahaman peserta sebesar 85%** yang ditunjukkan oleh lonjakan nilai rata-rata dari **45%** pada saat *pre-test* menjadi **83,25%** pada saat *post-test*. Peserta kini tidak hanya memahami aspek teoretis mengenai bahaya siber, melainkan juga memiliki keterampilan praktis dalam mengamankan akun media sosial, menjaga privasi data pribadi, mengenali modus kejahatan *phishing*, serta menyaring berita hoaks.

DAFTAR PUSTAKA

- Chandra, J., Tanaka, V., & Banke, R. (2025). Peran Interpol dalam menangani dan menanggulangi kejahatan siber di Indonesia. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 4(3), 4710-4719. <https://doi.org/10.56799/peshum.v4i3.9028>
- Djibu, M. A. (2025). Transformasi Digital dan Keamanan Siber: Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia. *Judge: Jurnal Hukum*, 6(01), 341-347. <https://doi.org/10.54209/judge.v6i01.1182>
- Dzaky, M. A. T., & Edrisy, I. F. (2025). Strategi pencegahan kejahatan siber di Indonesia: Sinergi antara UU ITE dan kebijakan keamanan digital. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora*, 4(2), 3614-3625. <https://doi.org/10.56799/peshum.v4i2.8311>
- Hidayat, S., & Radyawanto, A. S. (2025). KEMANDIRIAN SIBER INDONESIA: TANTANGAN DAN PELUANG MENUJU KEDAULATAN DIGITAL. *International Journal of Social and Management Studies*, 6(5), 98-102. <https://doi.org/10.5555/ijosmas.v6i5.537>
- Judijanto, L., & Nugroho, B. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrime di Indonesia. *Sanskara Hukum Dan HAM*, 3(03), 118-124. <https://doi.org/10.58812/shh.v3i03.544>
- Khaidir, A., Kurnia, M. P., & Erawaty, R. (2025). Perlindungan hukum terhadap korban kejahatan siber di Indonesia dalam perspektif hukum internasional. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6), 10563-10573. <https://doi.org/10.61104/alz.v3i6.2802>
- Maharani, M. A., & Atman, W. (2025). Evaluasi strategi nasional keamanan siber Indonesia dalam menanggapi ancaman digital Indonesia. *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik*, 2(3), 344-354. <https://doi.org/10.62383/sosial.v2i3.2291>
- Ramadhani, E. H., Enriko, I. K. A., & Sari, E. L. I. P. (2025). Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*, 6(1), 570-580. <https://doi.org/10.35870/jimik.v6i1.1210>