

Edukasi Keamanan Siber di SMK Kosgoro Bogor Sebagai Upaya Peningkatan Kesadaran dan Tanggung Jawab Digital Generasi Muda

Fahmi Nugraha Akbar¹, Aeni Syifa², Utari³, Faujan Faturahman⁴, Ahmad Rifai⁵, Ramlan Syahputra⁶, Revin Adrianus Tamsar⁷, Dicky Adiansyah Permana⁸, Muhammad Daniel Khaikal^{9*}, Muhammad Refa Fatur Rahman¹⁰

^{1,7}Sistem Informasi/Universitas Binaniaga Indonesia, Indonesia.

^{3,5,9,10}Teknik Informatika/Universitas Binaniaga Indonesia, Indonesia.

^{2,4,6,8}Teknologi Informasi/Universitas Binaniaga Indonesia, Indonesia.

fahmiakbr42305@gmail.com, aenisyf19@gmail.com, Utarinurrizki03@gmail.com,
fauzanfathur02@gmail.com, ahmdrifai808@gmail.com, ramlansyaputraaa@gmail.com,
revinadrianus01@gmail.com, dikipermana2254@gmail.com, danielsuleman.dk@gmail.com,
refafatur97@gmail.com

*) Corresponding author

ABSTRAK

Perkembangan teknologi digital yang semakin pesat menuntut generasi muda untuk memiliki kesadaran dan kemampuan yang memadai dalam menjaga keamanan data serta berperilaku secara bertanggung jawab di ruang siber. Namun, hasil observasi awal menunjukkan bahwa siswa SMK Kosgoro Bogor masih memiliki tingkat pemahaman yang rendah terkait ancaman siber, seperti phishing, pencurian data pribadi, malware, serta etika penggunaan media digital. Program pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi keamanan siber siswa melalui edukasi terstruktur yang mencakup penyuluhan teori, workshop simulasi phishing, diskusi interaktif, dan evaluasi berbasis kuesioner. Metode pelaksanaan terdiri atas presentasi dasar keamanan siber, praktik identifikasi ancaman digital melalui website phishing simulasi, serta game interaktif sebagai penguatan pemahaman. Hasil kegiatan menunjukkan peningkatan signifikan dari sisi pengetahuan dan kesadaran digital, dengan rata-rata pemahaman peserta mencapai 97,3% berdasarkan lima indikator utama, termasuk 100% pada aspek risiko berbagi informasi pribadi dan 97,7% pada pemahaman kata sandi kuat serta bahaya tautan mencurigakan. Selain itu, peserta menunjukkan perubahan perilaku positif seperti penerapan autentikasi dua faktor, peningkatan kewaspadaan pada link mencurigakan, serta pemahaman lebih baik terkait etika digital. Kegiatan ini membuktikan bahwa pendekatan edukasi yang interaktif dan aplikatif mampu meningkatkan kapasitas siswa dalam menghadapi ancaman siber serta mendorong terciptanya budaya keamanan digital di lingkungan sekolah.

Kata Kunci: Keamanan Siber; Literasi Digital; Phising; Edukasi; Pengabdian Masyarakat.

ABSTRACT

The rapid advancement of digital technology requires young generations to develop adequate awareness and competencies in protecting their data and behaving responsibly in cyberspace. However, initial observations indicate that students at SMK Kosgoro Bogor still have limited understanding regarding various cyberthreats such as phishing, data theft, malware, and ethical digital behavior. This community service program aims to enhance students' cybersecurity literacy through structured educational activities, including theoretical presentations, phishing simulation workshops, interactive discussions, and evaluation through questionnaires. The implementation methods consisted of cybersecurity awareness lectures, hands-on phishing

identification practice using a simulated phishing website, and interactive game-based learning to strengthen comprehension. The results show a significant improvement in students' knowledge and awareness, with an average understanding level reaching 97.3% across five key indicators, including 100% comprehension of personal data sharing risks and 97.7% understanding of strong password practices and suspicious link dangers. Furthermore, the program fostered positive behavioral changes such as the adoption of two-factor authentication, increased vigilance toward suspicious links, and improved digital ethics awareness. These outcomes indicate that interactive and practical cybersecurity education effectively enhances students' capabilities in responding to cyberthreats and contributes to building a stronger security culture within the school environment.

Keywords: Cyber Security; Digital Literacy; Phising; Education; Community Service.

PENDAHULUAN

Perkembangan teknologi digital yang pesat memberikan kemudahan dalam akses informasi dan komunikasi, namun juga meningkatkan risiko ancaman siber, khususnya bagi generasi muda. Berbagai penelitian menunjukkan bahwa pelajar sekolah menengah rentan terhadap penipuan daring, peretasan akun, serta penyalahgunaan data pribadi akibat rendahnya pemahaman keamanan digital (1). Studi internasional dan laporan tren global menegaskan bahwa remaja merupakan kelompok paling rentan karena intensitas penggunaan internet yang tinggi tanpa kecakapan literasi digital yang memadai (2).

Sejumlah penelitian membuktikan bahwa integrasi materi keamanan siber dalam pendidikan formal, terutama melalui metode pembelajaran interaktif seperti video, kuis, dan studi kasus, efektif meningkatkan kesadaran dan pemahaman siswa terhadap risiko digital (3)(4). Program literasi digital dan keamanan informasi yang diterapkan di berbagai sekolah di Indonesia juga menunjukkan dampak positif dalam mengurangi perilaku daring yang tidak aman serta meningkatkan kemampuan perlindungan data pribadi (5)(6).

Literasi keamanan siber tidak hanya penting bagi pelajar, tetapi juga bagi masyarakat secara umum dalam membangun budaya digital yang aman, etis, dan bertanggung jawab. Evaluasi literasi digital di tingkat komunitas menekankan perlunya pendekatan edukatif yang praktis dan partisipatif untuk meningkatkan kesadaran keamanan siber secara berkelanjutan (7).

SMK Kosgoro Bogor sebagai institusi pendidikan berbasis teknologi memiliki tingkat kerentanan yang relatif tinggi karena intensitas penggunaan perangkat digital dalam proses pembelajaran. Observasi awal menunjukkan bahwa meskipun siswa aktif menggunakan media digital, pemahaman mengenai keamanan siber, perlindungan data pribadi, dan tanggung jawab digital masih terbatas. Oleh karena itu, program pengabdian masyarakat bertema “Edukasi Keamanan Siber di SMK Kosgoro Bogor sebagai Upaya Meningkatkan Kesadaran dan Tanggung Jawab Digital Generasi Muda” diinisiasi untuk membekali siswa dengan pengetahuan dan keterampilan praktis dalam menghadapi ancaman siber serta membangun budaya digital yang aman dan bertanggung jawab.

METODE

Kegiatan Pengabdian Kepada Masyarakat (PkM) bertema “Edukasi Keamanan Siber di SMK Kosgoro Bogor sebagai Upaya Meningkatkan Kesadaran dan Tanggung

Jawab Digital Generasi Muda” dilaksanakan secara tatap muka pada tanggal 19 November 2025. Lokasi pelaksanaan bertempat di SMK Kosgoro Bogor, Jalan Raya Pajajaran No.217A, Kota Bogor. Pemilihan sekolah ini didasarkan pada hasil observasi awal yang menunjukkan tingginya kebutuhan siswa untuk meningkatkan literasi keamanan digital, terutama mengingat sekolah memiliki program keahlian yang erat dengan teknologi, seperti Komputer dan Jaringan, Rekayasa Perangkat Lunak, serta Desain Komunikasi Visual. Pelaksanaan kegiatan ini melibatkan dosen-dosen dari Fakultas Informatika dan Komputer Universitas Binaniaga Indonesia yang bertindak sebagai tim fasilitator dan edukator.

Metode pelaksanaan kegiatan dirancang menggunakan pendekatan edukasi yang terstruktur, interaktif, dan aplikatif dengan tujuan meningkatkan pengetahuan sekaligus mendorong perubahan perilaku positif siswa. Kegiatan dibagi ke dalam tiga fase utama, yaitu penyampaian teori, praktik simulasi, dan evaluasi hasil.

Tahap awal berupa penyuluhan teori yang mencakup presentasi mengenai dasar-dasar keamanan siber. Penyampaian materi dilakukan secara sistematis guna memastikan peserta memahami konsep dasar serta risiko nyata ancaman siber yang sering dihadapi pelajar. Pendekatan penyuluhan terstruktur ini terbukti efektif dalam meningkatkan literasi keamanan digital dan kesadaran siswa terhadap potensi serangan siber melalui penguatan pemahaman konseptual sebelum praktik lanjutan dilakukan (8). Materi yang disampaikan meliputi pengenalan berbagai ancaman digital seperti phishing, pencurian data pribadi, malware, serta pentingnya etika bermedia sosial. Selain itu, siswa juga diberikan pemahaman mengenai urgensi penggunaan kata sandi yang kuat dan penerapan Autentikasi Dua Faktor (Two-Factor Authentication/2FA).

Tahap berikutnya adalah workshop simulasi dan praktik, yang menjadi inti dari pendekatan aplikatif kegiatan PkM ini. Metode workshop digunakan untuk memberikan pengalaman langsung kepada siswa dalam mengenali, menganalisis, dan menanggapi berbagai bentuk ancaman siber. Kegiatan praktik terdiri atas simulasi phishing dan game interaktif keamanan digital, di mana siswa dilatih mengenali ciri-ciri tautan, email palsu, serta membedakan situs web yang aman dan berbahaya. Pendekatan pembelajaran berbasis praktik langsung telah terbukti efektif dalam memperkuat pemahaman peserta terhadap ancaman digital yang kompleks serta membangun keterampilan praktis dalam menghadapi kasus nyata di lingkungan digital (9).

Untuk memperkuat pemahaman, kegiatan workshop juga dilengkapi dengan diskusi dan sesi tanya jawab yang bersifat interaktif. Pada tahap ini, siswa diberikan ruang untuk berbagi pengalaman pribadi terkait permasalahan digital yang pernah mereka hadapi serta mendiskusikan solusi yang tepat. Penerapan elemen permainan dan interaksi aktif dalam pembelajaran literasi digital diketahui mampu meningkatkan motivasi, keterlibatan, dan daya serap siswa terhadap materi yang relatif kompleks (10).

Tahap terakhir adalah evaluasi dan penguatan pemahaman guna mengukur tingkat keberhasilan dan efektivitas program. Evaluasi dilakukan melalui kuesioner pre-test dan post-test untuk menilai peningkatan pengetahuan dan kesadaran siswa terhadap indikator utama keamanan siber. Selain itu, kuis cepat berbasis permainan digunakan sebagai metode penguatan untuk menguji retensi pemahaman siswa secara menyenangkan. Hasil evaluasi menunjukkan bahwa pendekatan edukasi yang interaktif dan berbasis praktik mampu meningkatkan kapasitas siswa dalam menghadapi ancaman siber serta mendorong terbentuknya budaya keamanan digital di lingkungan sekolah.

Melalui kombinasi metode penyuluhan, workshop praktik, diskusi interaktif, dan evaluasi berkelanjutan, diharapkan peningkatan literasi keamanan siber siswa SMK Kosgoro Bogor dapat tercapai secara efektif dan berkelanjutan.

HASIL DAN PEMBAHASAN

A). Sosialisasi dan Praktikum

Kegiatan dimulai dengan fase Sosialisasi dan Penyuluhan Teori yang bertujuan untuk membangun landasan pengetahuan yang kuat mengenai pentingnya keamanan siber. Sesi ini diawali dengan presentasi interaktif mengenai lanskap ancaman digital terkini. Tim pelaksana memaparkan secara rinci berbagai bentuk ancaman yang sering dihadapi oleh generasi muda, meliputi:

- 1) Phishing dan Social Engineering: Penjelasan mendalam tentang bagaimana pelaku kejahatan memanipulasi psikologi pengguna untuk mencuri data.
- 2) Risiko Data Pribadi: Pentingnya menjaga privasi, risiko data breach, serta konsekuensi hukum dan sosial dari penyebaran data sensitif.
- 3) Malware dan Peretasan Akun: Pengenalan jenis-jenis perangkat lunak berbahaya dan langkah-langkah pencegahan dasar.
- 4) Etika Digital (Netiket): Pembahasan mengenai tanggung jawab dalam berinteraksi di media sosial, menghindari cyberbullying, dan memverifikasi informasi untuk melawan hoax.

Metode penyampaian dilakukan secara dua arah, dengan melibatkan siswa dalam Diskusi Interaktif. Siswa didorong untuk berbagi pengalaman atau kasus ancaman siber yang pernah mereka temui, memungkinkan tim pelaksana memberikan solusi dan perspektif praktis secara langsung, sehingga materi terasa relevan dan mendesak untuk dipelajari.

Setelah pemahaman teori terbentuk, kegiatan dilanjutkan dengan tahap Workshop Simulasi dan Praktikum Aplikasi, di mana siswa dilibatkan dalam skenario nyata untuk mengasah keterampilan identifikasi dan pencegahan.

- 1) Praktik Identifikasi Phishing: Ini adalah fokus utama dari praktikum. Tim PkM menyiapkan website phishing simulasi yang aman dan terkontrol. Siswa diminta untuk menganalisis dan mengidentifikasi ciri-ciri tautan palsu, alamat Uniform Resource Locator (URL) yang mencurigakan, dan bahasa yang bersifat mendesak atau manipulatif dalam sebuah simulasi email. Latihan ini bertujuan agar siswa dapat membedakan mana sumber informasi yang aman dan mana yang berbahaya secara insting.
- 2) Pelatihan Keamanan Akun: Praktikum juga mencakup langkah-langkah konkret dalam pengamanan akun digital. Siswa dilatih tentang metodologi pembuatan kata sandi yang kuat dan unik, menghindari pola yang mudah ditebak. Yang lebih krusial, mereka dibimbing langkah demi langkah untuk mengaktifkan dan menggunakan Autentikasi Dua Faktor (2FA) pada akun-akun penting (seperti e-mail dan media sosial), menjadikannya sebagai praktik wajib dalam rutinitas digital mereka.

Kombinasi antara sosialisasi teoritis yang jelas dan praktikum simulasi yang aplikatif ini memastikan bahwa siswa tidak hanya mengerti konsep keamanan siber,

tetapi juga memiliki bekal keterampilan yang memadai untuk bertindak sebagai benteng pertahanan digital bagi diri mereka sendiri dan lingkungan sekolah.

B). Hasil yang diperoleh

Hasil kegiatan PkM menunjukkan peningkatan literasi keamanan siber yang signifikan pada siswa SMK Kosgoro Bogor, didukung oleh data kuantitatif dan perubahan perilaku kualitatif.

1) Peningkatan Pengetahuan

Evaluasi menggunakan pre-test dan post-test menunjukkan lonjakan drastis pada tingkat pemahaman siswa.

- a) Peningkatan Rata-Rata: Rata-rata pemahaman keseluruhan peserta meningkat ke tingkat yang sangat tinggi (mendekati 100%), menunjukkan bahwa edukasi terstruktur berhasil menjembatani kesenjangan pengetahuan awal.
- b) Fokus Kritis: Terjadi peningkatan terbesar dalam kemampuan mengidentifikasi tautan mencurigakan (phishing) dan pemahaman 100% pada risiko berbagi informasi pribadi, membuktikan efektivitas metode simulasi dan workshop praktis.

2) Perubahan Perilaku Positif

Program ini berhasil memicu perubahan kesadaran dan niat implementasi keamanan digital yang nyata.

- a) Penerapan Keamanan Akun: Peserta menunjukkan komitmen untuk segera menerapkan Autentikasi Dua Faktor (2FA) dan membuat kata sandi yang lebih kuat pada akun-akun penting mereka.
- b) Kewaspadaan Digital: Siswa kini lebih waspada terhadap tautan dan e-mail yang mencurigakan serta menunjukkan pemahaman yang lebih baik tentang etika digital dan tanggung jawab saat berinteraksi di dunia maya.

Secara keseluruhan, kegiatan ini membuktikan bahwa pendekatan edukasi yang interaktif dan aplikatif (melalui simulasi dan praktik) mampu meningkatkan kapasitas siswa dalam menghadapi ancaman siber dan berhasil mendorong terciptanya budaya keamanan digital yang kuat di lingkungan sekolah.



Gambar 1. Presentasi Penyuluhan



Gambar 2. Simulasi Phising



Gambar 3. Diskusi dan Tanya Jawab



Gambar 4. Game Interaktif

KESIMPULAN

Kegiatan ini berhasil mendorong perubahan perilaku positif, seperti penerapan Autentikasi Dua Faktor (2FA) dan peningkatan kewaspadaan terhadap tautan

mencurigakan. Dengan demikian, kegiatan ini tidak hanya meningkatkan kapasitas siswa dalam menghadapi ancaman siber, tetapi juga berkontribusi pada penciptaan budaya keamanan digital yang kuat di lingkungan sekolah.

UCAPAN TERIMA KASIH

Diucapkan terima kasih kepada para stakeholder dalam kegiatan PkM ini, diantaranya kepada Universitas Binaniaga Indonesia melalui LP3M yang dengan kesempatan yang diberikan sehingga dapat terlaksananya kegiatan ini, kepada Kepala Sekolah beserta kepala program SMK Kosgoro Bogor yang dengan tangan terbuka telah memberikan kesempatan kami untuk melaksanakan Tri Dharma Perguruan Tinggi yakni Pelaksanaan Pengabdian Kepada Masyarakat (PkM).

DAFTAR PUSTAKA

1. R. Apriani, S. Setiawan, T. Sudarsono, "SOSIALISASI DAN EDUKASI CYBER CRIME UNTUK MENINGKATKAN KESADARAN KEAMANAN DIGITAL," vol. 2.
2. M. A. A. A. et Al., "Measuring The Level of Cybersecurity Awareness of Social Media Users Among Students," *Seri Inform. INOVTEK Polbeng*, 2025, [Online]. Available: <https://jurnal.polbeng.ac.id/index.php/ISI/article/view/312>
3. A. A. Sussolaikah, R. D. Laksono, and M. Lenawati, "Pelatihan Keamanan Siber Guna Meningkatkan Literasi Digital di SMPN 14 Kota Madiun," *J. Abdimas Teknol. Inform. dan Komput.*, vol. 2, 2024, doi: <https://doi.org/10.31294/jatik.v1i2.3411>.
4. V. A. Tandirerung, R. T. Mangesa, and Syahrul, "Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas," *TEKNOVOKASI*, vol. 1, 2023.
5. M. Arifin, F. Helmi, and J. Dharmawan, "Peningkatan Literasi Digital Melalui Sosialisasi Pentingnya Pemahaman Kejahatan Siber Di Kalangan Pelajar SMAN 1 Gayam," *Rampa' Naong J. Pengabdi. Kpd. Masy.*, vol. 2, 2024.
6. A. K. Riski Arya Pratama, Noviyanti Santi, Anindya Putri, Nur Afifah, "Pengaruh Literasi Digital terhadap Perilaku Mahasiswa dalam Melindungi Data Pribadi dari Ancaman Siber," *J. Pustaka Nusantara. Multidisiplin*, vol. 3, 2025.
7. S. W. Dananjoyo, "LITERASI DIGITAL DI KALANGAN MASYARAKAT PEDESAAN: UPAYA MENINGKATKAN KESADARAN KEAMANAN SIBER," 2024, vol. 2.
8. E. D. W. Satria, J. Prayoga, "SOSIALISASI KEAMANAN SIBER BAGI PELAJAR DALAM MENGHADAPI ERA DIGITAL," *ABDI DALEM J. Pengabdi. Kpd. Masy.*, vol. 2, 2025.
9. T. S. R. Apriani, S. Sumardiono, S. Setiawan, "SOSIALISASI DAN EDUKASI CYBER CRIME UNTUK MENINGKATKAN KESADARAN KEAMANAN DIGITAL DAN CERDAS BERINTERNET BAGI SISWA," *J. Pengabdi. Masy. Ilmu Komput.*, vol. 2, 2025.
10. N. N. F. Ayuningtyas, M. Sakti, "PENINGKATAN KESADARAN LITERASI DIGITAL BAGI REMAJA MELALUI PROGRAM EDUKASI INTERAKTIF," *J. Abdimas Ilm. Citra Bakti*, vol. 6, 2025.