

Sosialisasi Keamanan Siber: Membangun Kesadaran Digital bagi Pelajar SMA Negeri 1 Dayeuhkolot

Kania Ayu Natya Lakshita Anpaduesta Ajid¹, Radiana De Salma¹, Ahmad Dzaky Ar Razi¹, Fahmi Septiano Shesta¹, Muhammad Rifqi Fauzani¹, Nikita Maulidya Edison¹, Yogi Anggun Saloko¹, Rio Guntur Utomo¹

¹Program Studi Sarjana Teknologi Informasi Fakultas Informatika, Telkom University, Jl. Telekomunikasi, Terusan Buahbatu, Bandung, Indonesia

email :

yogisaloko@telkomuniversity.ac.id, kaniaayu@student.telkomuniversity.ac.id,

radianade@student.telkomuniversity.ac.id,

dzakycok@student.telkomuniversity.ac.id,

fahmisshesta@student.telkomuniversity.ac.id,

muhammadrifqifauzan@student.telkomuniversity.ac.id,

nikitson@student.telkomuniversity.ac.id, yogisaloko@telkomuniversity.ac.id,

riogunturutomo@telkomuniversity.ac.id,

Abstrak/Abstract

Kegiatan “Sosialisasi Cyber Security untuk Pelajar” merupakan program pengabdian masyarakat yang bertujuan untuk meningkatkan pemahaman dasar pelajar SMA terhadap isu-isu keamanan siber. Kegiatan ini dilaksanakan di SMA Negeri 1 Dayeuhkolot dan menyasar siswa kelas 10 yang dianggap masih memiliki pengetahuan terbatas terkait ancaman dunia digital. Sosialisasi dilakukan secara tatap muka dalam dua sesi, masing-masing terdiri dari pre-test, pemaparan materi, dan post-test. Materi yang disampaikan meliputi pengertian keamanan siber, jenis-jenis ancaman, cara pencegahan, serta pentingnya perlindungan data pribadi. Hasil evaluasi menunjukkan bahwa kegiatan berjalan lancar dan mendapat respons positif dari peserta. Terdapat peningkatan pemahaman peserta yang signifikan, terlihat dari hasil post-test dan antusiasme saat sesi diskusi. Peserta menjadi lebih sadar akan risiko di dunia maya dan menunjukkan ketertarikan untuk mempelajari topik lebih lanjut. Kegiatan ini dinilai berhasil mencapai tujuan yang ditetapkan dan dapat dijadikan model untuk pelaksanaan sosialisasi keamanan siber di lingkungan sekolah lainnya.

Kata kunci: keamanan siber, pelajar, sosialisasi, literasi digital, data pribadi

1. METODE PENGABDIAN

Di era digital saat ini, internet telah menjadi bagian tak terpisahkan dari kehidupan manusia. Aktivitas sehari-hari seperti belajar, bekerja, berkomunikasi, bahkan hiburan dilakukan melalui jaringan internet. Meskipun memberikan banyak manfaat, kemajuan teknologi informasi juga membawa tantangan besar, salah satunya adalah meningkatnya ancaman terhadap keamanan siber. Pelajar sebagai generasi muda yang sangat aktif menggunakan teknologi digital menjadi salah satu kelompok yang rentan terhadap serangan siber. Hal ini disebabkan karena minimnya pemahaman mereka tentang pentingnya menjaga keamanan data pribadi dan cara menghadapi ancaman digital.

Badan Siber dan Sandi Negara (BSSN) melaporkan bahwa pada tahun 2022 terdapat lebih dari 1,6 juta kasus serangan siber di Indonesia. Jumlah ini meningkat 20% dibandingkan tahun sebelumnya, mencerminkan adanya tren ancaman yang terus

berkembang di berbagai sektor, termasuk pendidikan. Ancaman ini tidak hanya bersifat teknis tetapi juga menyasar aspek psikologis dan sosial dari penggunaannya, seperti phishing, rekayasa sosial, dan penyebaran malware melalui media sosial yang sering digunakan pelajar.

Lebih dari 95% insiden siber disebabkan oleh kesalahan manusia, yang dapat diminimalkan melalui edukasi dan peningkatan kesadaran pengguna (Bulai, Turcanu, & Ciorba, 2022). Pendidikan keamanan siber dinilai sebagai investasi terbaik dalam mencegah berbagai serangan digital. Pendekatan terbaik untuk melindungi pengguna dari serangan siber adalah dengan menggabungkan teknologi dan edukasi yang menyeluruh. Dalam konteks pendidikan, lembaga sekolah memiliki tanggung jawab membentuk budaya digital yang aman melalui pembelajaran perilaku online yang bijak.

Menurut Khalidov (2024), institusi pendidikan menghadapi tantangan yang signifikan dalam menangani ancaman digital, sehingga penting untuk mengintegrasikan kurikulum keamanan siber ke dalam sistem pendidikan. Pengetahuan ini perlu diajarkan sejak usia dini karena siswa dan staf sekolah merupakan bagian integral dari ekosistem digital yang perlu dilindungi.

Kegiatan “Sosialisasi Cyber Security untuk Pelajar” hadir sebagai upaya konkret untuk memberikan pemahaman dasar mengenai ancaman dan pencegahan siber kepada pelajar SMA Negeri 1 Dayeuhkolot. Dengan metode interaktif berupa pre-test dan post-test, kegiatan ini diharapkan menjadi media edukasi efektif yang dapat membentuk kesadaran baru tentang pentingnya perlindungan data digital bagi generasi muda.

Musina dan Gilmanov (2024) juga menekankan perlunya pendekatan lintas disiplin dalam mengedukasi keamanan siber serta pentingnya kerja sama antara institusi pendidikan, pemerintah, dan sektor industri. Hal ini sejalan dengan pendapat Shoemaker dan Kohnke (2016) yang menyatakan bahwa pendidikan adalah agen perubahan sosial paling efektif dalam meningkatkan ketahanan terhadap ancaman dunia maya. Tanpa fondasi pendidikan yang kuat, masyarakat akan terus menjadi target empuk bagi para penjahat siber.

Ahmad, Laplante, DeFranco, dan Kassab (2022) menambahkan bahwa pendidikan keamanan siber harus dijadikan bagian dari kurikulum wajib di semua tingkat pendidikan agar terbentuk komunitas digital yang tangguh dan sadar akan risiko.

Berdasarkan latar belakang tersebut, kegiatan ini dilaksanakan dengan nama **"Sosialisasi Cyber Security untuk Pelajar"**, dengan **tema** utama menyampaikan materi edukatif seputar ancaman dan pencegahan serangan siber yang relevan dengan kehidupan pelajar sekolah menengah atas.

Sasaran kegiatan ini adalah siswa kelas 10 SMA Negeri 1 Dayeuhkolot, yang merupakan pengguna aktif internet dan berisiko tinggi terhadap ancaman digital. Tujuan dari kegiatan ini meliputi:

1. Memberikan pemahaman dasar tentang keamanan siber kepada pelajar.
2. Meningkatkan kesadaran pelajar tentang ancaman digital dan pentingnya menjaga privasi.

3. Menjadikan pelajar sebagai agen perubahan dalam menyebarkan budaya digital yang aman di lingkungan sekolah dan masyarakat.

Dengan terlaksananya kegiatan ini, diharapkan pelajar tidak hanya menjadi pengguna teknologi yang aktif, tetapi juga bijak dan bertanggung jawab dalam menjaga keamanan dirinya dan lingkungannya dari berbagai ancaman digital yang ada.

2. METODE PENGABDIAN

2.1 Konsep Kegiatan

Kegiatan "Sosialisasi Cyber Security untuk Pelajar" dirancang untuk memberikan pemahaman dasar mengenai keamanan siber kepada pelajar SMA, khususnya kelas 10 di SMA Negeri 1 Dayeuhkolot. Model pelaksanaan dilakukan secara tatap muka dan interaktif dengan memanfaatkan metode pembelajaran aktif berupa sesi tanya jawab, diskusi, serta pre-test dan post-test untuk mengukur peningkatan pemahaman peserta.

Pendekatan ini selaras dengan prinsip bahwa pendidikan merupakan investasi paling bijak dalam upaya meningkatkan kesadaran terhadap keamanan digital, terutama karena 95% insiden keamanan berasal dari kesalahan manusia (Bulai dkk., 2022). Maka dari itu, penguatan aspek pendidikan menjadi solusi utama dalam mengurangi kerentanan pelajar terhadap serangan siber.

Kegiatan ini juga diharapkan mendorong pembentukan komunitas pelajar yang memiliki kesadaran akan risiko digital, sebagaimana direkomendasikan oleh beberapa studi bahwa literasi siber sebaiknya ditanamkan sejak pendidikan dasar hingga universitas untuk menciptakan budaya aman digital yang berkelanjutan (Ahmad dkk., 2022).

2.2. Materi Pembahasan

Materi yang disampaikan dalam sosialisasi ini mencakup lima aspek penting dalam dunia keamanan siber. Pertama, pengenalan mengenai apa itu keamanan siber, termasuk definisinya, ruang lingkup, dan pentingnya topik ini dalam kehidupan digital. Kedua, jenis-jenis ancaman yang umum dihadapi oleh pengguna internet, seperti phishing, malware, dan kebocoran data pribadi melalui media sosial. Ketiga, tindakan preventif yang dapat dilakukan untuk mencegah serangan siber, seperti penggunaan kata sandi yang kuat, tidak membagikan informasi pribadi secara sembarangan, dan menjaga kerahasiaan akun. Keempat, langkah-langkah yang dapat dilakukan jika terjadi serangan, termasuk pelaporan dan upaya pemulihan. Terakhir, manfaat dari memiliki wawasan keamanan siber yang baik, seperti meningkatkan kesadaran digital, membentuk etika bermedia, dan menjadi agen perubahan yang dapat menyebarluaskan kesadaran tersebut kepada orang lain.

Metode penyampaian materi dirancang untuk menyentuh aspek kognitif dan afektif peserta. Seperti yang dijelaskan dalam studi sebelumnya, integrasi pendekatan aktif seperti diskusi, permainan edukatif, dan pemodelan situasi nyata dapat secara signifikan meningkatkan minat pelajar terhadap keamanan siber (Triplett, 2023). Selain itu, pendidikan keamanan siber yang dimulai sejak jenjang sekolah terbukti menjadi fondasi yang kuat dalam membangun budaya informasi dan kesadaran digital jangka panjang (Bolun et al., 2021).

2.3 Target Luaran

Target dari kegiatan ini tidak hanya berfokus pada kuantitas peserta, tetapi lebih pada pencapaian peningkatan kualitas pemahaman mereka terhadap topik keamanan siber. Kegiatan ini melibatkan sekitar 60 pelajar dari dua kelas yang berbeda. Diharapkan setelah mengikuti kegiatan ini, pelajar memiliki pemahaman yang lebih baik mengenai ancaman digital dan cara menghadapinya, yang diukur melalui hasil post-test. Selain itu, keterlibatan aktif peserta dalam sesi tanya jawab menjadi indikator bahwa kegiatan ini mampu merangsang rasa ingin tahu mereka terhadap isu yang dibahas.

Lebih jauh, kegiatan ini juga bertujuan membentuk pelajar sebagai agen perubahan di lingkungan sekitarnya. Dengan pemahaman yang mereka peroleh, peserta diharapkan dapat menyebarkan informasi mengenai pentingnya keamanan digital kepada teman sebaya maupun keluarga. Konsep ini selaras dengan gagasan bahwa pendidikan keamanan siber bukan hanya untuk membentuk individu yang paham teknologi, tetapi juga menciptakan masyarakat digital yang sadar risiko dan mampu menjaga diri di dunia maya (Ahmad dkk., 2022). Dukungan terhadap pendekatan edukasi lintas disiplin dan inklusif juga disampaikan oleh (Shoemaker & Kohnke, 2016), yang menyatakan bahwa pendidikan yang menyentuh aspek sosial dan perilaku digital sangat penting untuk menciptakan ketahanan siber yang menyeluruh.

Pada bagian metode penerapan, uraikanlah dengan jelas dan padat metode yang digunakan untuk mencapai tujuan yang telah dicanangkan dalam kegiatan pengabdian. Hasil pengabdian itu harus dapat diukur dan penulis diminta menjelaskan alat ukur yang dipakai, baik secara deskriptif maupun kualitatif. Jelaskan cara mengukur tingkat ketercapaian keberhasilan kegiatan pengabdian. Tingkat ketercapaian dapat dilihat dari sisi perubahan sikap, sosial budaya, dan ekonomi masyarakat sasaran.

3. HASIL DAN PEMBAHASAN

3.1. Pelaksanaan Kegiatan

Kegiatan “Sosialisasi Cyber Security untuk Pelajar” dilaksanakan pada hari Senin, tanggal 20 November 2023, bertempat di SMA Negeri 1 Dayeuhkolot, Kabupaten Bandung. Sosialisasi ini ditujukan bagi siswa kelas 10-3 dan 10-6, dan berlangsung dari pukul 12.45 hingga 15.20 WIB. Pelaksanaan kegiatan terbagi ke dalam dua sesi untuk masing-masing kelas.

Kegiatan dimulai dengan persiapan panitia dan registrasi peserta, kemudian dilanjutkan dengan pembukaan acara dan sambutan dari pihak sekolah. Setelah itu, dilakukan sesi pre-test melalui ice breaking untuk mengetahui sejauh mana pemahaman awal peserta terkait keamanan siber. Materi sosialisasi kemudian disampaikan secara interaktif oleh panitia yang bertindak sebagai pemateri, dilanjutkan dengan sesi post-test guna mengukur peningkatan pemahaman peserta. Kegiatan ditutup dengan doa bersama.

Dalam pelaksanaannya, panitia juga melakukan identifikasi dan mitigasi terhadap berbagai risiko yang mungkin terjadi, seperti keterlambatan jadwal, ketidakhadiran pembicara, hingga kendala teknis seperti mati listrik. Solusi atas risiko tersebut telah dirancang sebelumnya guna menjaga kelancaran acara. Kegiatan ini dilaksanakan oleh tim yang terdiri dari enam orang mahasiswa, dengan pembagian tugas mencakup ketua tim, pemateri, MC, dokumentasi, dan penanggung jawab multimedia.

3.2 Hasil Kegiatan

Kegiatan sosialisasi cyber security berlangsung dengan lancar dan sesuai dengan rencana yang telah ditetapkan dalam rundown acara. Sosialisasi ini diikuti oleh total 58 peserta dari dua kelas, yaitu kelas 10-3 dan 10-6 SMA Negeri 1 Dayeuhkolot.

Selama pelaksanaan, peserta menunjukkan antusiasme tinggi, khususnya dalam sesi tanya jawab dan ice breaking. Pada awal kegiatan, mayoritas peserta belum memahami konsep dasar keamanan siber, termasuk ancaman dan cara penanggulangannya. Namun, setelah pemberian materi, terdapat peningkatan yang signifikan dalam pemahaman mereka, sebagaimana terlihat dari hasil post-test dan keterlibatan aktif dalam diskusi. Materi yang disampaikan mencakup pengertian keamanan siber, jenis-jenis ancaman siber, langkah-langkah pencegahan, serta peran penting pelajar dalam menjaga keamanan data pribadi di era digital. Para peserta juga diberi pemahaman mengenai tindakan yang harus diambil jika menghadapi serangan siber.

Kegiatan ini tidak hanya memberikan wawasan baru, tetapi juga mendorong peserta untuk menjadi agen perubahan dalam menyebarkan kesadaran tentang keamanan siber kepada lingkungan sekitar. Beberapa siswa bahkan menyampaikan bahwa mereka tertarik untuk mempelajari keamanan siber lebih lanjut di luar kegiatan ini.



Gambar 1. Dokumentasi Kegiatan

Secara keseluruhan, kegiatan berjalan sesuai dengan tujuan yang telah dirumuskan sebelumnya, yaitu untuk meningkatkan pemahaman dasar pelajar mengenai keamanan siber dan menciptakan kesadaran kolektif terhadap pentingnya menjaga informasi pribadi di ruang digital. Keberhasilan pelaksanaan ini menjadi dasar yang kuat untuk pengembangan kegiatan serupa di masa mendatang, baik di sekolah yang sama maupun di institusi pendidikan lainnya.

4. KESIMPULAN

Kegiatan “Sosialisasi Cyber Security untuk Pelajar” yang dilaksanakan di SMA Negeri 1 Dayeuhkolot berhasil terlaksana dengan baik dan sesuai dengan rencana. Tujuan utama kegiatan, yaitu memberikan pemahaman dasar mengenai keamanan siber kepada pelajar kelas 10, telah tercapai dengan adanya peningkatan pengetahuan yang signifikan dari peserta berdasarkan hasil pre-test dan post-test.

Sosialisasi ini juga mampu meningkatkan kesadaran peserta terhadap berbagai ancaman di dunia digital, seperti pencurian data, penipuan online, dan pentingnya menjaga kerahasiaan informasi pribadi. Dengan metode penyampaian yang interaktif dan partisipatif, kegiatan ini tidak hanya menyampaikan materi, tetapi juga membangun keterlibatan aktif dari para peserta.

Dari hasil evaluasi, kegiatan ini memiliki potensi besar untuk dikembangkan lebih lanjut, baik dalam bentuk pelatihan lanjutan maupun perluasan sasaran ke sekolah-sekolah lain. Peserta menunjukkan antusiasme tinggi dan sebagian besar menyatakan ketertarikan untuk memperdalam wawasan mereka dalam bidang keamanan siber.

5. SARAN

Agar kegiatan serupa dapat berjalan lebih optimal di masa mendatang, beberapa saran yang dapat diberikan adalah:

1. Menambah durasi waktu untuk sesi diskusi agar peserta dapat lebih leluasa dalam menyampaikan pendapat dan pertanyaan.
2. Menyediakan materi dalam bentuk digital agar dapat diakses ulang oleh peserta setelah kegiatan.
3. Melibatkan narasumber eksternal dari praktisi keamanan siber untuk memperkaya sudut pandang peserta.

Dengan demikian, diharapkan kegiatan ini menjadi langkah awal yang berkelanjutan dalam meningkatkan literasi digital dan kesadaran keamanan siber di kalangan pelajar.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Telkom University yang telah memberi dukungan terhadap keberhasilan pengabdian ini.

DAFTAR PUSTAKA

Ahmad, N. B., Laplante, P., DeFranco, J., & Kassab, M. (2022). *A cybersecurity educated community*. IEEE Transactions on Emerging Topics in Computing, 10, 1456–1463.

Bolun, I., Bulai, R., & Ciorba, D. (2021). *Support of education in cybersecurity*. Pro Publico Bono – Magyar Közigazgatás.

Bulai, R., Turcanu, D., & Ciorba, D. (2022). *Education in cybersecurity*. Central and Eastern European eDem and eGov Days.

Shoemaker, D., & Kohnke, A. (2016). *Cyber education and the emerging profession of cybersecurity*. EDPACS, 54(1), 12–16.

Triplett, W. J. (2023). *Addressing cybersecurity challenges in education*. International Journal of STEM Education for Sustainability.

Khalidov, A. A. (2024). *Cybersecurity in educational environment: Training and practice*. EKONOMIKA I UPRAVLENIE: PROBLEMY, RESHENIYA.

Musina, L. F., & Gilmanov, I. M. (2024). *Cybersecurity in education: Training and practice*. EKONOMIKA I UPRAVLENIE: PROBLEMY, RESHENIYA.