

Sosialisasi Membangun Generasi Tangguh Melawan Kejahatan Cyber pada SMK Plus Krida Utama Padalarang

Ade Yuliana

Politeknik TEDC Bandung, Cimahi, Indonesia
e-mail: yulianaad@poltektedc.ac.id

Novita Lestari Anggreini

Politeknik TEDC Bandung, Cimahi, Indonesia
e-mail: novitalestari@poltektedc.ac.id

Castaka Agus Sugianto

Politeknik TEDC Bandung, Cimahi, Indonesia
e-mail: castaka@poltektedc.ac.id

Heldi Akbar Kosasih

Politeknik TEDC Bandung, Cimahi, Indonesia
e-mail: heldiakbar999@gmail.com

Abstract

Abstract: This community service program aims to improve digital literacy and cybersecurity awareness among vocational high school students at SMK Plus Krida Utama Padalarang. The increasing threat of cybercrimes such as phishing, hacking, malware, and cyberbullying poses significant risks to students who are often active but underprepared digital users. Through interactive workshops, real-life case studies, and quizzes, the program successfully enhanced students' understanding of cyber threats and prevention strategies. The sessions focused on practical steps like using strong passwords, recognizing suspicious links, managing online privacy, and practicing safe digital behavior. Evaluation results indicated increased student engagement and awareness, demonstrating the importance of early cybersecurity education. The outcomes suggest that structured and relatable digital safety training is effective in building resilience against cybercrime among young users.

Keywords— Digital Literacy, Cybersecurity Awareness, Vocational Students, Phishing, Cybercrime Prevention

1. PENDAHULUAN

Di era digital saat ini, penggunaan internet dan platform digital telah menjadi bagian integral dari kehidupan sehari-hari, termasuk bagi pelajar Sekolah Menengah Kejuruan (SMK). Meskipun memberikan berbagai kemudahan, peningkatan konektivitas ini juga diiringi dengan berbagai ancaman siber yang semakin kompleks, seperti penipuan daring (*phishing*) dan pencurian data (Dinas Pendidikan Jawa Barat, 2023). Banyak siswa SMK, yang merupakan generasi digital *native*, seringkali memiliki pemahaman yang terbatas mengenai risiko-risiko

ini serta cara melindungi diri mereka secara efektif di dunia maya. Menurut Sanatang et al., (2021), kurangnya literasi digital yang komprehensif dan kesadaran keamanan siber dapat mengakibatkan siswa rentan menjadi korban kejahatan siber atau secara tidak sengaja terlibat dalam aktivitas daring yang tidak aman.

Penelitian menunjukkan bahwa program kesadaran keamanan siber yang komprehensif dapat secara signifikan mengurangi insiden terkait keamanan dan meningkatkan kemampuan individu dalam mengenali serta merespons ancaman siber. Menurut Kristianti et al., (2024) menyatakan bahwa upaya edukasi keamanan siber yang terstruktur sangat efektif dalam mengurangi risiko kejahatan siber. Oleh karena itu, Program Pengabdian Kepada Masyarakat (PkM) ini bertujuan untuk meningkatkan literasi digital dan kesadaran keamanan siber siswa SMK, khususnya di SMK Plus Krida Utama. Melalui edukasi yang terstruktur dan praktis, diharapkan siswa dapat memiliki pemahaman yang lebih baik tentang risiko daring dan mampu menerapkan praktik keamanan siber dalam kehidupan digital mereka. Program ini berfokus pada penyampaian pengetahuan dasar tentang keamanan siber, identifikasi ancaman umum, serta praktik terbaik dalam menjaga privasi dan data pribadi di ranah digital.

2. METODE

Kegiatan Pengabdian kepada Masyarakat ini merupakan bagian dari pelaksanaan Tri Dharma Perguruan Tinggi yang diinisiasi oleh dosen Politeknik TEDC Bandung dengan melibatkan mahasiswa sebagai bagian dari proses pembelajaran berbasis pengalaman. Kegiatan ini menggunakan pendekatan sosialisasi yang interaktif dan partisipatif, dengan materi yang disusun secara kontekstual berdasarkan kebutuhan dan karakteristik siswa SMK sebagai sasaran utama.

Dalam pelaksanaannya, dosen berperan sebagai fasilitator utama yang memandu jalannya pelatihan, menyampaikan materi utama, serta mengarahkan diskusi untuk memperkuat pemahaman peserta. Mahasiswa turut mendukung kegiatan ini secara aktif, baik dalam penyusunan materi, dokumentasi, maupun menjadi narasumber tambahan yang berbagi pengalaman langsung terkait penggunaan teknologi digital serta langkah-langkah preventif yang mereka terapkan dalam menghadapi ancaman kejahatan siber.

Rangkaian kegiatan dilakukan secara sistematis melalui tiga tahapan utama: (1) perencanaan dan pengembangan konten pelatihan, (2) pelaksanaan kegiatan sosialisasi secara langsung, dan (3) evaluasi dampak serta penyusunan laporan kegiatan. Kolaborasi ini tidak hanya memberi kontribusi nyata bagi masyarakat, tetapi juga menjadi wahana penguatan kapasitas akademik dan praktis mahasiswa melalui keterlibatan langsung dalam kegiatan pengabdian yang diinisiasi oleh dosen.

2.1 Perencanaan dan Persiapan

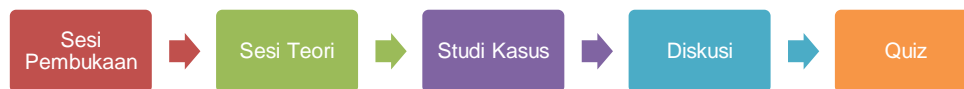
Fase perencanaan dan persiapan ini mencakup identifikasi masalah melalui survei awal atau wawancara dengan pihak sekolah dan siswa untuk memahami tingkat literasi digital dan kesadaran keamanan siber. Materi presentasi disusun dan media pendukung (*poster*, *power point*) yang mudah dipahami dibuat. Materi disesuaikan untuk mencakup topik-topik krusial seperti pengenalan ancaman siber (*phishing*, *malware*), pentingnya kata sandi yang kuat, privasi data online, etika digital, dan cara merespons insiden keamanan.

2.2 Pelaksanaan Pelatihan

Kegiatan ini dilakukan dalam bentuk sosialisasi yang melibatkan sesi penyampaian materi interaktif, studi kasus, diskusi, dan penyampaian motivasi Yuliana et al., (2025).

- Sesi Pembukaan: Berisi sambutan, pengenalan tim, dan penjelasan tujuan program untuk membangun suasana yang kondusif.
- Sesi Teori/Materi: Penyampaian konsep kejahatan cyber, disertai dengan contohnya yaitu *Phishing*, *Hacking*, *Malware* dengan dipaparkan analoginya. Selain itu, terdapat materi *cyber bullying*.
- Studi Kasus: Analisis contoh kasus kejahatan siber yang relevan dengan pengalaman siswa. Peserta diajak untuk mengidentifikasi email atau pesan *phishing* palsu untuk melatih kewaspadaan mereka. Pada *cyber bullying* disampaikan akan dampak terhadap korban, dan seluruh kejahatan cyber dilengkapi dengan cara mencegahnya.
- Diskusi: Sesi interaktif untuk tanya jawab dan pembahasan topik-topik keamanan akun digital, termasuk panduan langkah demi langkah dalam mengamankan akun media sosial dan email, serta penggunaan otentikasi multi-faktor (MFA).
- Quiz: Pelaksanaan kuis interaktif untuk mengukur pemahaman siswa terhadap materi yang telah disampaikan dan memperkuat proses pembelajaran.

Rangkaian kegiatan ini berkolaborasi antara dosen dan mahasiswa dalam sesi penyampaian materi, studi kasus, diskusi dimana alur pelaksanaan dapat dilihat pada Gambar 1 berikut ini.



Gambar 1. Pelaksanaan Kegiatan

2.3 Luaran Kegiatan

Luaran utama dari kegiatan ini adalah peningkatan literasi digital dan kesadaran keamanan siber di kalangan siswa-siswi SMK Plus Krida Utama. Melalui pendekatan edukatif yang interaktif, peserta diharapkan mampu mengenali berbagai bentuk kejahatan siber seperti *phishing* dan *malware*, memahami dampaknya, serta mempraktikkan langkah-langkah perlindungan digital seperti penggunaan kata sandi yang kuat, pengaturan privasi, dan kehati-hatian dalam aktivitas daring. Selain meningkatkan pemahaman teknis, kegiatan ini juga bertujuan menumbuhkan keterlibatan aktif siswa dalam forum edukatif dan membentuk agen perubahan yang dapat menyebarluaskan pengetahuan keamanan digital di lingkungan sekolah dan sekitarnya.

Kegiatan ini dilaksanakan oleh dosen sebagai pelaksana utama pengabdian kepada masyarakat yang merancang dan mengarahkan seluruh tahapan kegiatan, mulai dari penentuan topik, penyusunan strategi penyampaian materi, hingga pelaksanaan dan evaluasi. Mahasiswa dilibatkan sebagai pendukung aktif, khususnya dalam menyampaikan materi dari perspektif generasi Z yang relevan dan mudah diterima oleh siswa SMK. Dengan gaya komunikasi yang lebih dekat secara kultural dan generasional, mahasiswa mampu membangun jembatan komunikasi yang efektif dalam menjelaskan isu-isu teknologi dan keamanan digital.

Sebagai bentuk nyata pelaksanaan Tri Dharma Perguruan Tinggi, kegiatan ini menghasilkan luaran dokumentatif berupa laporan kegiatan dan artikel ilmiah. Dalam proses ini, dosen memegang peran sebagai pembimbing akademik yang memastikan kualitas isi dan kontribusi keilmuan dari kegiatan pengabdian. Luaran

tersebut tidak hanya berfungsi sebagai bukti tanggung jawab sosial institusi, tetapi juga sebagai sarana reflektif dan referensi bagi pengembangan program sejenis di masa mendatang.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Kegiatan

Hasil kegiatan pengabdian kepada masyarakat dilaksanakan secara *offline* pada tanggal 14 Januari 2025, pukul 08.00 – 10.55 WIB bertempat di SMK Plus Krida Utama Padalarang. Partisipasi Peserta yang hadir pada kegiatan pengabdian sebanyak 23 orang yang terdiri dari 11 siswa-siswi kelas XI DKV, dan 12 siswa-siswi kelas XI PB SMK Plus Krida Utama Padalarang.

Table 1. Susunan Acara

No	Waktu	Jenis Kegiatan	PJ
1	06:00-07:30	Kumpul Panitia dan menyiapkan Konsumsi	Seluruh Panitia
2	07.30-08.00	Menyiapkan Logistik yang dibutuhkan dan berangkat menuju Lokasi	Seluruh Panitia
3	08:00-08:30	Registrasi peserta dan Persiapan Panitia	Peserta dan Panitia
4	08:30-08:45	Pembukaan acara dan Sambutan	MC
5	08:45-09.45	Penyampaian Materi	Pemateri
6	09:45-10.00	Ice Breaking dan Game	MC
7	10.00-10.30	Games dan Quiz Interaktif	MC
8	10.30-10:45	Penutupan Acara	MC
9	10.45-10.55	Dokumentasi	Seluruh Panitia

Berikut dokumentasi kegiatan Pengabdian ini yang mencakup tahapan pembukaan, pelaksanaan, hingga penutupan.



Gambar 2. Pembukaan Kegiatan

Pada Gambar 2 terlihat sedang berlangsung agenda pertama yaitu pembukaan yang diawali dengan pengenalan, sambutan, dan penjelasan agenda sosialisasi.



Gambar 3. Pemaparan Materi Sosialisasi

Pada Gambar 3 sedang berlangsung agenda inti yaitu penyampaian konsep kejahatan cyber, disertai dengan contohnya yaitu *Phishing*, *Hacking*, *Malware* dengan dipaparkan analoginya. Selain itu, terdapat materi *cyber bullying*.



Gambar 4. Penyampaian contoh Studi Kasus

Pada Gambar 4 peserta mendapatkan studi kasus atas materi yang disampaikan, juga dijelaskan mengenai dampak yang didapatkan, dan juga cara pencegahannya agar hal tersebut tidak terjadi di lingkungan kita.



Gambar 5. Sesi Tanya Jawab kepada Siswa

Gambar 5 merupakan sesi tanya jawab yang disampaikan dari siswa kepada pemateri tentang materi, dan yang berkaitan dengan kejahatan cyber.



Gambar 6. Diskusi dengan Siswa mengenai Materi

Gambar 6 sedang berlangsung kegiatan diskusi antara siswa dengan mahasiswa penyelenggara kegiatan sosialisasi. Diskusi ini mengenai materi yang disampaikan, terdapat pertanyaan dan pernyataan seputar kejahatan *cyber* di kehidupan sehari-hari, dan cara mencegahnya.



Gambar 7. Sesi Quiz dan Games

Gambar 7 merupakan sesi quiz seputar materi yang disampaikan, dan hal-hal yang berkaitan dengan kejahatan *cyber* di lingkungan kita. Selain itu terdapat games, games ini bertujuan untuk meningkatkan keakraban mahasiswa dengan siswa agar mendapatkan interaksi yang akrab dan positif.



Gambar 8. Penyerahan hadiah pemenang quiz, games dan pertanyaan terbaik

Gambar 8 merupakan apresiasi yang diberikan dari penyelenggara sosialisasi terhadap siswa yang aktif memberikan pertanyaan terbaik, serta memberikan hadiah atas pemenang quiz, dan juga games.



Gambar 9. Foto Bersama dan Penutupan

Gambar 9 dokumentasi foto Bersama antara seluruh panitia, dosen, penyelenggara dengan siswa sebagai peserta sosialisasi ini.

3.2 Pembahasan

Materi yang disampaikan oleh mahasiswa Politeknik TEDC Bandung pada agenda sosialisasi di SMK Plus Krida Utama Padalarang yaitu mengenai kejahatan cyber, berikut pemaparan materinya.



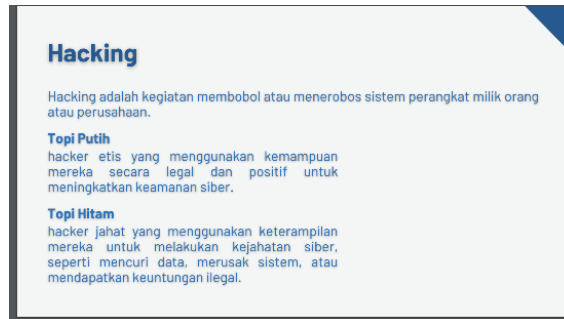
Gambar 10. Mengenalkan Apa itu Kejahatan Cyber?

Pada Gambar 10 menjelaskan materi awal yang disampaikan yaitu tentang kejahatan cyber, kejahatan cyber merupakan aktivitas yang dilakukan di dunia digital menggunakan perangkat teknologi seperti computer atau smartphone (Habibi & Liviani, 2020).



Gambar 11. Penjelasan tentang Phishing

Pada Gambar 11 penyampaian materi mengenai Pishing yang merupakan kejahatan siber yang dilakukan untuk menipu dan mendapatkan data sensitive pengguna (Dewanto et al., 2024).



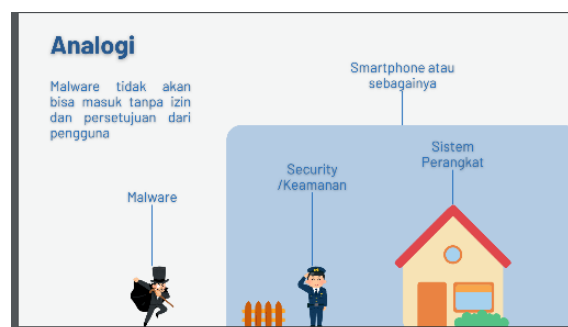
Gambar 12. Penjelasan tentang Hacking

Gambar 12 penjelasan materi Hacking yang merupakan kegiatan membobol atau menerobos system perangkat milik orang atau perusahaan. Terdapat Hacker topi putih yaitu hacker etis yang melakukan secara positif dan legal, lalu topi Hitam yaitu hacker jahat yang menggunakan skill nya untuk kejahatan cyber (Widyarto & Hapsari, 2022).



Gambar 13. Penjelasan tentang Malware

Gambar 13 penyampaian mengenai Malware yang merupakan perangkat lunak yang telah dirancang untuk merusak system, mencuri data, dan lain sebagainya. Terdapat juga macam macam malware dan virus (Sianipar & Pangaribuan, 2023).



Gambar 14. Analogi dari Malware

Gambar 14 merupakan Analogi dari Malware itu sendiri, penjelasan analogi ini untuk memudahkan mahasiswa dalam memahami cara kerja Malware.



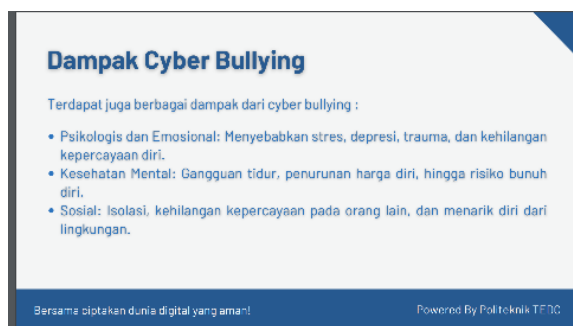
Gambar 15. Dampak Pishing, Hacking, dan Malware

Gambar 15 penjelasan langsung mengenai dampak yang akan terjadi pada korban Pishing yaitu data pribadi dicuri, kerugian finansial, lalu Hacking akan mengakibatkan kehilangan data berharga, ancaman dan gangguan privasi, Malware mengakibatkan kerusakan perangkat, pencurian data, ransomware. (Azzahra et al., 2024).



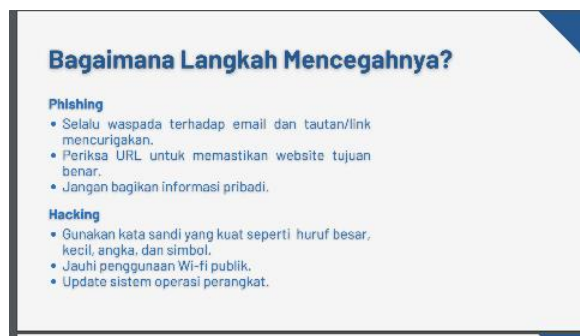
Gambar 16. Pengertian Cyber Bullying

Gambar 16 memaparkan materi tentang Cyber Bullying, cyber bullying ini merupakan Tindakan perundungan yang sering terjadi secara online atay pada dunia maya, kegiatan ini merupakan perilaku berukang yang ditujukan untuk menakuti, membuat marah, dan memperlakukan mereka yang menjadi sasaran (Imani et al., 2021).



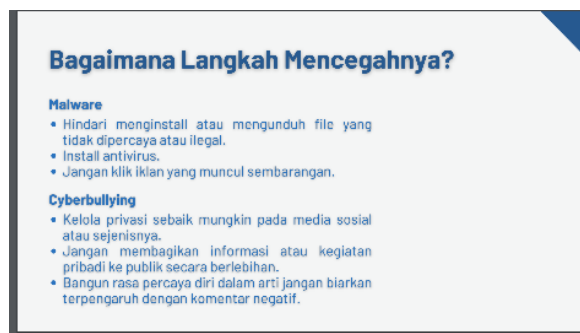
Gambar 17. Dampak dari Cyber Bullying

Gambar 17 merupakan materi mengenai dampak pada Cyber bullying itu sendiri, diantaranya yaitu gangguan psikologis dan emosional, Kesehatan mental, dan kehilangan kepercayaan orang lain atau gangguan social (Ni'mah, 2023).



Gambar 18. Langkah pencegahan Phishing, Hacking

Gambar 18 adalah penyampaian materi mengenai Bagaimana Langkah untuk mencegah Phishing dan Hacking, Untuk pencegahan Phishing yaitu harus selalu waspada terhadap email dan tautan/link mencurigakan, jangan bagikan informasi pribadi. Untuk Hacking yaitu gunakan kata sandi yang kuat dan tidak mudah diingat atau dihafal orang lain, jauhi penggunaan wi-fi publik, dan selalu update system operasi perangkat (Aabid et al., 2025).



Gambar 19. Langkah pencegahan Malware dan Cyberbullying

Gambar 19 adalah lanjutan dari Gambar 18 mengenai Bagaimana Langkah Mencegah kejahatan cyber, dijelaskan mengenai Langkah mencegah Malware dan CyberBullying. Langkah yang telah dijelaskan oleh mahasiswa kepada siswa sosialisasi ini sangat membuka pemikiran siswa agar tetap berhati-hati dan waspada agar terhindar dari kejahatan cyber.

4. KESIMPULAN

Kegiatan pengabdian kepada masyarakat yang dilaksanakan oleh dosen dan mahasiswa Politeknik TEDC Bandung di SMK Plus Krida Utama Padalarang menunjukkan efektivitas nyata dalam meningkatkan literasi digital dan kesadaran keamanan siber di kalangan siswa. Melalui pendekatan edukatif yang interaktif dan kontekstual, siswa dibekali pemahaman mendasar tentang risiko dunia maya, termasuk jenis-jenis ancaman seperti *phishing*, *malware*, serta dampaknya terhadap privasi dan keamanan data pribadi.

Program ini difokuskan pada penguatan pemahaman siswa terhadap prinsip-prinsip dasar keamanan siber dan praktik preventif yang dapat diterapkan dalam kehidupan digital sehari-hari. Respons peserta menunjukkan antusiasme tinggi: mereka aktif berdiskusi, merefleksikan pengalaman digitalnya, serta mulai menerapkan langkah-langkah perlindungan seperti penggunaan autentikasi yang aman, pengaturan privasi, dan peningkatan kewaspadaan terhadap tautan atau

informasi mencurigakan. Hal ini menandakan tumbuhnya kesadaran kritis terhadap potensi kejahatan digital, sekaligus kesiapan untuk menjadi pengguna internet yang lebih cerdas dan bertanggung jawab.

Sebagai bagian dari implementasi Tri Dharma Perguruan Tinggi, kegiatan ini dipimpin oleh dosen sebagai fasilitator utama yang merancang, membimbing, dan menyampaikan materi inti, dengan dukungan mahasiswa yang turut memperkuat penyampaian melalui sudut pandang generasi muda yang dekat dengan realitas siswa SMK. Kolaborasi ini tidak hanya menghasilkan dampak sosial yang terukur, tetapi juga melahirkan luaran akademik berupa dokumentasi kegiatan dan artikel ilmiah, yang memperkuat kontribusi institusi dalam pengembangan pengetahuan dan pengabdian berkelanjutan di bidang literasi digital dan keamanan siber.

5. SARAN

Agar dampak jangka panjang dapat tercapai, disarankan agar pendidikan mengenai keamanan siber dimasukkan ke dalam kurikulum sekolah secara berkelanjutan. Dukungan dari institusi pendidikan, pemerintah, dan sektor swasta sangat diperlukan untuk mengadakan pelatihan dan kampanye kesadaran digital secara berkala. Program lanjutan dapat melibatkan pendekatan *peer-to-peer* agar keterlibatan siswa tetap tinggi serta membentuk budaya sadar keamanan digital yang berkelanjutan di kalangan generasi muda.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada POLITEKNIK TEDC BANDUNG atas dukungan finansial dan fasilitas yang telah diberikan untuk terlaksananya program pengabdian ini. Apresiasi juga disampaikan kepada SMK Plus Krida Utama, khususnya para guru dan siswa yang telah berpartisipasi aktif dalam kegiatan ini.

DAFTAR PUSTAKA

- Aabid, M., Dzaky, T., & Fikma Edrisy, I. (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
- Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). Tinjauan Literatur Tentang Ancaman Cybercrime Dan Implementasi Keamanan Siber Di Industri Perbankan . *HUMANITIS: Jurnal Humaniora, Sosial Dan Bisnis*, 2(7), 692–700.
- Dewanto, M. A. B., Fathurrahman, M., Firdaus, D. R., & Setiawan, A. (2024). Penipuan penambah followers Instagram: Analisis serangan phishing dan dampaknya pada keamanan data. *Journal of Internet and Software Engineering*, 1(4), 1–11
- Dinas Pendidikan Jawa Barat. (2023). Modul Literasi Digital untuk Pelajar SMK. Bandung: Dinas Pendidikan Jawa Barat
- Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal*

- Pemikiran Dan Pembaharuan Hukum Islam*, 23(2), 400–426.
<https://doi.org/10.15642/alqanun.2020.23.2.400-426>
- Imani, F. A., Kusmawati, A., & Amin, H. M. T. (2021). Pencegahan Kasus Cyberbullying Bagi Remaja Pengguna Sosial Media. *Khidmat Sosial: Journal of Social Work and Social Services*, 2(1), 74–83.
- Kristianti, N., Kurniasi, R., Raya, U. P., & Jurnal, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Jurnal Ilmu Hukum*, 6055(1), 297–310.
- Ni'mah, S. A. (2023). Pengaruh Cyberbullying pada Kesehatan Mental Remaja. *Prosiding Seminar Nasional Bahasa, Sastra Dan Budaya (SEBAYA) Ke-3*, 329–338.
- Sanatang, Lamada, M., Rahayu, N., & Dewi, S. S. (2021). Pelatihan Literasi Digital Bagi Siswa Sekolah Menengah Kejuruan Negeri 2 Makassar. *IPTEK : Jurnal Hasil Pengabdian Masyarakat*, 1(2), 119–127.
- Sianipar, V. R., & Pangaribuan, H. (2023). Analisis Dan Deteksi Malware Pada Protokol Jaringan Menggunakan Metode Malware Analisis Dinamis Dan Malware Analisis Statis. *Computer and Science Industrial Engineering (COMASIE)*, 9(6), 790–797.
- Widyarto, E. Y., & Hapsari, D. K. (2022). Analisis Modus Operandi Tindak Kejahatan Menggunakan Teknik Komunikasi Love Scam Sebagai Ancaman pada Keamanan Sistem Informasi. *Syntax Idea*, 4(9), 1352.
- Yuliana, A., Sugianto, C. A., Anggreini, N. L., & Rismayana, A. H. (2025). Sosialisasi bahaya dan cara aman menggunakan WiFi publik pada Karang Taruna Komplek Nusa Hijau. *JPPkM: Jurnal Pengabdian dan Pemberdayaan kepada Masyarakat*, 1(1), 12–19.