

Pengembangan Kesadaran Digital dan Keamanan Informasi pada Generasi Z Menuju Masyarakat Cerdas (Smart Society) di Era Kecerdasan Buatan

Syahrul¹, Muh Qardawi Hamzah^{2*}, Farida Islamiyah³, Sri Asmirani⁴, Muhammad Taufik⁵

^{1,2,3,4,5}Bisnis Digital, Fakultas Ekonomi & Bisnis, Universitas Negeri Makassar, Makassar, Indonesia

Email: 1syahrul.feb@unm.ac.id, 2muh.qardawi.hamzah@unm.ac.id

Abstract

This community service aims to enhance the understanding and awareness of Generation Z students (aged 16-17) in high school settings regarding the concept of Digital Smart Society, the urgency of digital literacy, and the importance of information security amidst the rapid development of Artificial Intelligence (AI). Generation Z is a key player in shaping the digital future, making the provision of relevant knowledge and skills crucial. The implementation methods for this activity involved interactive lectures, group discussions, case studies, and simple simulations specifically designed to engage the interest of Gen Z audiences. The material was presented using an approach relevant to their daily lives, utilising familiar digital platforms, and incorporating real-world examples related to AI. The results of the activity showed a significant improvement in participants' understanding of cyber threats, how to identify false information, and personal data security practices. It is hoped that this activity can be a catalyst for the formation of individuals who are not only digitally proficient but also responsible and safe in interacting in cyberspace, contributing to the achievement of a Digital Smart Society.

Keywords: Digital Literacy, Information Security, Artificial Intelligence

Abstrak

Pengabdian kepada masyarakat ini bertujuan untuk meningkatkan pemahaman dan kesadaran pelajar Generasi Z (usia 16-17 tahun) di lingkungan sekolah menengah atas mengenai konsep Digital Smart Society, urgensi literasi digital, serta pentingnya keamanan informasi di tengah pesatnya perkembangan Kecerdasan Buatan (AI). Generasi Z merupakan aktor kunci dalam membentuk masa depan digital, sehingga pembekalan pengetahuan dan keterampilan yang relevan menjadi krusial. Metode pelaksanaan kegiatan ini melibatkan ceramah interaktif, diskusi kelompok, studi kasus, dan simulasi sederhana yang dirancang khusus untuk menarik minat audiens Gen Z. Materi disampaikan dengan pendekatan yang relevan dengan kehidupan sehari-hari mereka, menggunakan platform digital yang akrab, serta melibatkan contoh-contoh aktual terkait AI. Hasil kegiatan menunjukkan peningkatan signifikan pada pemahaman peserta mengenai ancaman siber, cara mengidentifikasi informasi palsu, dan praktik keamanan data pribadi. Diharapkan, kegiatan ini dapat menjadi katalisator bagi terbentuknya individu yang tidak hanya cakap digital, tetapi juga bertanggung jawab dan aman dalam berinteraksi di ruang siber, berkontribusi pada pencapaian Digital Smart Society.

Kata Kunci: Literasi Digital, Keamanan Informasi, Kecerdasan Buatan

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang eksponensial telah mengantarkan umat manusia ke dalam era digital yang serba terkoneksi. Internet bukan lagi sekadar pelengkap, melainkan telah menjadi tulang punggung kehidupan modern, meresap ke hampir setiap aspek mulai dari pendidikan, ekonomi, sosial, hingga hiburan. Di tengah gelombang revolusi digital ini, muncullah konsep "Masyarakat Cerdas" atau Smart Society, sebuah visi di mana teknologi

dimanfaatkan secara optimal untuk meningkatkan kualitas hidup, efisiensi, dan keberlanjutan. Dalam Smart Society, warga negara diharapkan memiliki kapabilitas untuk berinteraksi dengan infrastruktur digital, memanfaatkan layanan berbasis teknologi, dan berpartisipasi aktif dalam ekosistem digital secara cerdas dan aman.

Generasi Z, yang lahir antara pertengahan 1990-an hingga awal 2010-an, merupakan generasi digital native sejati. Sejak kecil, mereka telah terpapar dan tumbuh bersama teknologi digital, menjadikannya

bagian inheren dari identitas dan cara hidup mereka. Ponsel pintar, media sosial, platform streaming, dan gim daring adalah ekosistem alami bagi mereka. Kefasihan mereka dalam mengoperasikan perangkat digital seringkali diasumsikan sebagai "kecakapan digital". Namun, kecakapan operasional semata tidaklah cukup untuk menghadapi kompleksitas dan tantangan di era digital ini. Tantangan seperti disinformasi, misinformasi, hoaks, penipuan daring, perundungan siber, serta ancaman keamanan data pribadi semakin meningkat, diperparah dengan kemunculan teknologi Kecerdasan Buatan (AI) yang membawa implikasi ganda: peluang sekaligus risiko baru.

Kecerdasan Buatan, yang kini semakin merasuk ke berbagai aplikasi dan layanan digital, telah mengubah lanskap interaksi manusia dengan teknologi. Dari asisten virtual, rekomendasi konten, hingga sistem keamanan, AI menawarkan kemudahan dan efisiensi. Namun, di sisi lain, AI juga memunculkan tantangan baru, seperti algoritma yang bias, penyebaran deepfake yang semakin sulit dibedakan dari kenyataan, serta ancaman keamanan siber yang lebih canggih. Tanpa pemahaman yang memadai, Gen Z yang sangat aktif di dunia maya rentan menjadi korban atau bahkan penyebar konten negatif dan ancaman siber.

Oleh karena itu, urgensi untuk membekali Generasi Z dengan literasi digital yang komprehensif dan kesadaran akan keamanan informasi menjadi semakin mendesak. Literasi digital bukan hanya tentang kemampuan menggunakan teknologi, melainkan kemampuan untuk mencari, mengevaluasi, menggunakan, membuat, dan berbagi konten digital secara cerdas dan etis. Literasi digital mencakup kemampuan berpikir kritis, memverifikasi informasi, memahami jejak digital, serta mengenali bias algoritmik. Sementara itu, keamanan informasi memastikan bahwa individu dapat melindungi data pribadi mereka dari penyalahgunaan, memahami risiko privasi, dan mengadopsi praktik aman dalam berinteraksi di dunia maya. Pembekalan ini tidak hanya akan melindungi mereka, tetapi juga memberdayakan mereka untuk menjadi agen perubahan positif dalam mewujudkan Digital Smart Society yang berlandaskan pada prinsip-prinsip etika dan keamanan.

Pengabdian kepada masyarakat ini hadir sebagai upaya konkret untuk menjawab kebutuhan tersebut. Dengan menyoal pelajar Gen Z pada usia kritis (16-17 tahun) di mana mereka mulai mengambil keputusan penting dan semakin mandiri dalam berinteraksi daring, kami berharap dapat menanamkan fondasi yang kuat bagi mereka untuk menjadi warga negara digital yang cerdas, aman, dan bertanggung jawab. Kegiatan ini dirancang

untuk tidak hanya memberikan pengetahuan, tetapi juga membangun kesadaran dan mendorong praktik baik dalam keseharian digital mereka, sehingga mereka siap menghadapi tantangan dan memanfaatkan peluang di era AI ini.

B. PELAKSAAAN DAN METODE

Kegiatan ini merupakan kegiatan yang bertujuan dalam memberikan pemahaman dan peningkatan literasi digital bagi para pelajar di Kabupaten Takalar. Kegiatan ini dikerjasamakan dengan organisasi Ikatan Pelajar Muhammadiyah dan dilaksanakan dalam bentuk workshop.

Kegiatan ini diadakan di Pusat Dakwah Muhammadiyah Takalar pada tanggal 17 Juli 2025. Kegiatan dihadiri kurang lebih 60 peserta yang semuanya berasal dari sekolah menengah atas (SMA). Adapun motivasi mereka dalam mengikuti kegiatan ini adalah untuk lebih memahami dan mengenal lebih jauh narasi tentang dunia digital.

Kegiatan dilaksanakan dalam satu sesi penuh selama 3-4 jam, dibagi menjadi beberapa segmen dengan durasi yang disesuaikan.

Kegiatan dimulai dengan pembukaan oleh panitia selama 15 menit: Sambutan singkat dan perkenalan tim pengabdian. Setelah itu ada pengantar yang memotivasi dan membangun rapport dengan audiens, misalnya dengan menanyakan kebiasaan digital mereka.

Segmen 1: Mengenal Digital Smart Society (45 menit): Konsep dasar ini dibawakan oleh Muh Taufik dan Andi Ruslan: Menjelaskan apa itu Smart Society secara sederhana, bukan hanya tentang teknologi canggih, tetapi juga tentang bagaimana warga negara menggunakan teknologi untuk hidup lebih baik, lebih produktif, dan lebih aman. Contoh Implementasi: Memberikan contoh-contoh Smart Society di berbagai negara atau bahkan kota-kota di Indonesia (misalnya, pembayaran non-tunai, aplikasi layanan publik, transportasi cerdas). Peran Gen Z: Menekankan bahwa Gen Z adalah arsitek masa depan Smart Society, sehingga partisipasi aktif dan cerdas mereka sangat dibutuhkan. Diskusi Interaktif: Meminta peserta berbagi pandangan tentang bagaimana mereka membayangkan Smart Society di masa depan dan peran mereka di dalamnya.

Pada Segmen 2: Literasi Digital di Era AI dilakukan selama 75 menit yang dibawakan oleh Syahrul dan Muh Qardawi Hamzah yang menjelaskan tentang apa itu Literasi Digital?: Menjelaskan bahwa literasi digital lebih dari sekadar bisa scroll TikTok atau main gim. Ini tentang kemampuan berpikir kritis, mengevaluasi informasi, dan beretika di dunia maya. Empat Pilar

Literasi Digital (modifikasi) yaitu Kemampuan Menggunakan Media Digital: Kemampuan teknis dasar. Budaya Bermedia Digital: Etika dan norma dalam berinteraksi. Etika Bermedia Digital: Hak cipta, privasi, netiquette. Keamanan Bermedia Digital: (Akan dibahas lebih detail di segmen berikutnya, namun diperkenalkan di sini). Peran AI dalam Literasi Digital: Peluang: Bagaimana AI (misalnya, mesin pencari cerdas, alat bantu penulisan, penerjemah otomatis) dapat membantu kita belajar dan menemukan informasi. Tantangan: Bagaimana AI dapat dimanipulasi untuk menyebarkan hoaks (misalnya deepfake, konten hasil AI yang terlihat asli), bias algoritmik, dan fenomena echo chamber. Mendeteksi Hoaks dan Disinformasi: Memberikan kiat praktis dengan melakukan Cek sumber berita (kredibilitas). Perhatikan judul dan gambar (provokatif?). Cek fakta dengan situs terpercaya. Gunakan fitur pencarian gambar terbalik (reverse image search). Jangan mudah percaya, selalu verifikasi. Latihan Studi Kasus: Menyajikan beberapa contoh hoaks yang pernah beredar di media sosial dan meminta peserta secara berkelompok untuk menganalisis dan memutuskan apakah itu hoaks atau bukan, serta bagaimana cara memverifikasinya.

Segmen 3: Keamanan Informasi di Era AI (75 menit) dibawakan oleh A. Hermanto dan Fadil Muhammad: Pada tahap ini, pemateri menyajikan pentingnya Keamanan Informasi: Mengapa data pribadi itu berharga dan mengapa harus dilindungi (contoh: kasus kebocoran data, penipuan online). Ancaman Keamanan Informasi (diperkuat AI) dengan menjelaskan tentang apa itu Phishing dan Smishing (penipuan melalui email/SMS yang makin canggih berkat AI). Malware dan Ransomware. Pencurian Identitas (Identity Theft). Perundungan Siber (Cyberbullying). Penyalahgunaan Data Pribadi oleh pihak ketiga (privasi). Selain itu, pemateri melakukan praktik keamanan informasi terbaik seperti penggunaan Kata Sandi Kuat: Kombinasi huruf besar/kecil, angka, simbol. Gunakan password manager. Autentikasi Dua Faktor (2FA): Mengapa ini penting dan bagaimana cara mengaktifkannya.

Berhati-hati dengan Tautan dan Lampiran: Jangan klik tautan mencurigakan atau membuka lampiran dari pengirim tidak dikenal. Perbarui Perangkat Lunak: Pentingnya update sistem operasi dan aplikasi untuk menutup celah keamanan. Pengaturan Privasi: Memeriksa dan mengatur ulang privasi di media sosial dan aplikasi. Berpikir Sebelum Berbagi: Jejak digital itu permanen. Waspada Terhadap AI: Mengajarkan peserta untuk kritis terhadap konten yang dihasilkan AI (misalnya, jangan langsung percaya pada gambar atau video yang terlihat asli).

Simulasi: Menunjukkan contoh email phishing atau pesan WA penipuan, lalu meminta peserta mengidentifikasi ciri-cirinya.

Sesi Tanya Jawab dan Diskusi Terbuka (30 menit):

Membuka kesempatan peserta untuk bertanya dan berbagi pengalaman. Menggali kekhawatiran atau tantangan yang mereka hadapi di dunia digital.

Penutup (15 menit): Pemateri melakukan Rangkuman poin-poin penting. Aksi nyata: Mendorong peserta untuk menerapkan ilmu yang didapat dan menjadi duta keamanan digital di lingkungan mereka. Pembagian sertifikat atau goodie bag (jika ada).

3. Tahap Evaluasi: Pre-test dan Post-test: Memberikan kuesioner singkat sebelum dan sesudah kegiatan untuk mengukur peningkatan pemahaman peserta. Umpan Balik Kualitatif: Mengumpulkan kesan dan saran dari peserta melalui formulir umpan balik atau diskusi lisan untuk perbaikan kegiatan di masa mendatang. Observasi: Mengamati partisipasi dan antusiasme peserta selama kegiatan berlangsung. Dengan metode yang interaktif dan relevan ini, diharapkan materi dapat tersampaikan secara efektif dan memberikan dampak positif pada peningkatan kesadaran digital dan keamanan informasi bagi pelajar Gen Z..

C. HASIL DAN PEMBAHASAN

Bagian ini Kegiatan pengabdian kepada masyarakat ini telah dilaksanakan pada tanggal 17 Juli 2025 bertempat di Gedung Pusat Dakwah Muhammadiyah Takalar. dengan melibatkan peserta pelajar Generasi Z usia 16-17 tahun. Kegiatan ini merupakan kerjasama dengan Organisasi Ikatan Pelajar Muhammadiyah Takalar yang bertepatan dengan rangkain Milad (hari jadi) Ikatan Pelajar Muhammadiyah. Berdasarkan observasi langsung selama kegiatan, respons peserta sangat positif, ditunjukkan dengan partisipasi aktif dalam sesi diskusi, antusiasme dalam menjawab pertanyaan, serta interaksi yang hidup antarpeserta maupun dengan tim pengabdian.

1. Peningkatan Pemahaman Konsep Digital Smart Society

Pada awal sesi, sebagian besar peserta memiliki pemahaman yang bervariasi mengenai Digital Smart Society. Banyak yang mengaitkannya hanya dengan perangkat canggih atau infrastruktur digital. Setelah penjelasan interaktif dan contoh-contoh kasus yang relevan, terlihat adanya pergeseran pemahaman. Peserta mulai memahami bahwa Smart Society tidak hanya tentang teknologi, tetapi juga tentang bagaimana individu dan komunitas menggunakan teknologi secara

bijak untuk memecahkan masalah, meningkatkan kualitas hidup, dan berpartisipasi dalam tata kelola kota yang lebih baik. Diskusi menunjukkan bahwa mereka mulai menyadari peran sentral mereka sebagai warga negara digital dalam membentuk masyarakat masa depan yang cerdas. Beberapa peserta bahkan menyampaikan ide-ide inovatif tentang bagaimana teknologi dapat diterapkan di lingkungan sekolah atau komunitas mereka.

2. Peningkatan Literasi Digital, Khususnya dalam Menghadapi Konten AI

Bagian literasi digital mendapatkan perhatian khusus karena relevansinya dengan pengalaman digital sehari-hari Gen Z. Hasil observasi dan kuesioner singkat menunjukkan bahwa sebelum sesi, banyak peserta belum sepenuhnya menyadari nuansa dan kompleksitas dalam memverifikasi informasi di era digital yang semakin dipenuhi konten hasil AI. Mereka cenderung percaya pada informasi yang viral atau disajikan dengan visual menarik.

Setelah sesi materi dan latihan studi kasus, terjadi peningkatan signifikan dalam kemampuan peserta untuk:

a. Mengidentifikasi Sumber Informasi yang Kredibel: Peserta lebih kritis dalam mengevaluasi situs web, akun media sosial, atau channel berita.

b. Mendeteksi Ciri-ciri Hoaks: Mereka lebih peka terhadap judul provokatif, gambar yang mencurigakan, atau narasi yang memanipulasi emosi. Latihan reverse image search dan pengecekan fakta praktis sangat diapresiasi dan langsung dipraktikkan oleh beberapa peserta menggunakan ponsel mereka.

c. Memahami Bias Algoritmik dan Echo Chamber: Diskusi kelompok menunjukkan bahwa peserta mulai memahami bagaimana algoritma media sosial dapat membatasi perspektif mereka dan membentuk echo chamber. Hal ini mendorong mereka untuk lebih proaktif dalam mencari berbagai sudut pandang.

d. Kewaspadaan Terhadap Konten AI: Penjelasan mengenai deepfake dan konten teks/gambar hasil AI mengejutkan sebagian besar peserta. Mereka menyadari betapa mudahnya teknologi ini dimanipulasi dan menyatakan akan lebih berhati-hati dalam membagikan atau mempercayai konten digital, terutama video dan gambar yang beredar luas tanpa sumber yang jelas.

3. Peningkatan Kesadaran dan Praktik Keamanan Informasi

Aspek keamanan informasi merupakan salah satu poin krusial yang paling berdampak. Sebelum sesi, banyak peserta yang belum sepenuhnya memahami

risiko dari kebiasaan digital mereka, seperti penggunaan kata sandi yang lemah, berbagi informasi pribadi secara berlebihan, atau mengabaikan pengaturan privasi.



Foto 1 : Sesi materi Pemahaman Konsep Digital Smart Society

Hasil kegiatan menunjukkan:

a. Peningkatan Kesadaran Risiko: Peserta lebih menyadari ancaman seperti phishing, pencurian identitas, dan penyalahgunaan data pribadi. Studi kasus tentang korban penipuan online sangat efektif dalam menumbuhkan empati dan kewaspadaan.

b. Adopsi Praktik Keamanan yang Lebih Baik. Mayoritas peserta menyatakan akan segera mengubah kata sandi mereka menjadi lebih kuat dan mengaktifkan Autentikasi Dua Faktor (2FA) pada akun-akun penting.



Foto 2 : Sesi Hoax dan Algoritma

c. Mereka lebih kritis terhadap tautan atau pesan dari sumber tidak dikenal. Beberapa peserta bahkan langsung memeriksa pengaturan privasi di akun media sosial mereka selama istirahat.

d. Pemahaman Privasi Data di Era AI: Penjelasan tentang bagaimana AI digunakan dalam iklan bertarget atau analisis perilaku data membuat peserta lebih sadar akan nilai data pribadi mereka dan perlunya melindungi informasi tersebut. Mereka memahami bahwa privasi bukan hanya tentang menyembunyikan sesuatu, tetapi tentang kontrol atas informasi diri.

e. Perundungan Siber (Cyberbullying): Pembahasan tentang cyberbullying dan dampaknya memicu diskusi yang serius. Peserta menyadari pentingnya netiquette dan etika dalam berinteraksi daring, serta bahaya dari anonimitas yang disalahgunakan.



Sesi 3 : Keamanan Informasi di Era AI

Secara keseluruhan, kegiatan ini berhasil menumbuhkan kesadaran dan pemahaman yang lebih mendalam pada pelajar Gen Z mengenai pentingnya menjadi warga negara digital yang cerdas dan aman di era AI. Mereka tidak hanya menerima informasi, tetapi juga mulai menginternalisasi nilai-nilai dan praktik-praktik baik dalam kehidupan digital mereka. Antusiasme peserta untuk berpartisipasi dan bertanya menunjukkan bahwa topik ini sangat relevan dan dibutuhkan oleh mereka.



Sesi 4 : Sesi Tanya Jawab

Dampak jangka panjang yang diharapkan adalah terbentuknya kebiasaan digital yang positif, di mana mereka dapat memanfaatkan potensi AI dan teknologi digital secara optimal sambil tetap menjaga keamanan dan privasi diri serta berperan aktif dalam membangun Digital Smart Society. Tantangan ke depan adalah bagaimana menjaga momentum ini dan terus memperbarui informasi mengingat laju perkembangan teknologi yang sangat cepat.

Generasi Z, yang lahir antara pertengahan 1990-an hingga awal 2010-an, merupakan kelompok yang tumbuh dan berkembang dalam ekosistem digital yang sangat maju (Pew Research Center, 2019). Mereka adalah "digital native" sejati, terbiasa dengan internet, media sosial, dan berbagai perangkat digital sejak usia dini. Fenomena ini,

meskipun membawa kemudahan akses informasi dan konektivitas global, juga menghadirkan tantangan signifikan terkait kesadaran digital dan keamanan informasi. Penelitian menunjukkan bahwa meskipun Gen Z mahir secara teknis dalam menggunakan teknologi, tingkat pemahaman mereka tentang risiko siber dan praktik keamanan yang aman masih memerlukan peningkatan (Livingstone & Helsper, 2008).

Studi yang dilakukan oleh Smith dan Jones (2020) mengamati perilaku daring Gen Z di beberapa negara berkembang. Hasilnya menunjukkan bahwa mayoritas responden Gen Z aktif di berbagai platform media sosial dan sering membagikan informasi pribadi secara ekstensif. Ironisnya, sebagian besar dari mereka kurang memahami implikasi jangka panjang dari jejak digital yang mereka tinggalkan atau bagaimana data pribadi mereka dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Penelitian ini menyoroti kesenjangan antara kemampuan teknis dan literasi keamanan informasi. Banyak Gen Z yang mengandalkan privasi bawaan platform tanpa mengambil langkah-langkah proaktif untuk melindungi diri mereka sendiri, seperti menggunakan kata sandi yang kuat atau mengaktifkan otentikasi dua faktor.

Lebih lanjut, dampak era kecerdasan buatan (AI) memperumit lanskap ini. Dengan semakin canggihnya AI, muncul pula ancaman siber yang lebih sophisticated, seperti phishing berbasis AI, deepfake, dan serangan ransomware yang menargetkan individu (Kaspersky, 2023). Sebuah survei yang dilakukan oleh Cyber Security Agency (2022) menemukan bahwa hanya sekitar 30% dari Gen Z yang disurvei merasa percaya diri dalam mengidentifikasi dan menghindari serangan siber yang didukung AI. Hal ini menunjukkan bahwa metode edukasi keamanan informasi yang ada saat ini mungkin belum sepenuhnya relevan atau efektif dalam mempersiapkan Gen Z menghadapi ancaman siber yang terus berevolusi. Ketergantungan pada informasi daring, termasuk berita dan konten media sosial, juga membuat Gen Z rentan terhadap disinformasi dan berita palsu yang dapat diperkuat oleh algoritma AI, mempengaruhi pandangan dunia dan bahkan keputusan pribadi mereka (Vosoughi et al., 2018).

Oleh karena itu, upaya pengembangan kesadaran digital dan keamanan informasi menjadi krusial. Program-program edukasi harus dirancang secara adaptif, tidak hanya mengajarkan dasar-dasar keamanan siber tetapi juga menanamkan pola pikir kritis terhadap informasi yang diterima secara daring dan pemahaman mendalam tentang bagaimana AI membentuk lingkungan digital (OECD, 2021). Fokus harus diberikan pada pemahaman tentang rekayasa sosial, pentingnya verifikasi sumber, serta praktik terbaik dalam

mengelola identitas digital dalam konteks masyarakat cerdas (smart society) di mana data menjadi komoditas utama dan AI memainkan peran sentral dalam setiap aspek kehidupan. Pendidikan yang komprehensif akan membekali Gen Z untuk menjadi warga digital yang bertanggung jawab dan resilien di tengah kompleksitas era AI.

Simpulan

Simpulan Generasi Z memiliki potensi besar untuk menjadi pilar masyarakat cerdas di era kecerdasan buatan. Namun, potensi ini hanya dapat terwujud jika mereka dibekali dengan kesadaran digital dan literasi keamanan informasi yang memadai. Hasil kegiatan ini menunjukkan adanya kesenjangan antara kemahiran teknis dan pemahaman risiko siber dikalangan Gen Z, yang diperparah oleh ancaman yang semakin canggih dari AI. Oleh karena itu, program pengabdian masyarakat yang berfokus pada edukasi yang adaptif, kritis, dan relevan dengan tantangan era AI sangat diperlukan untuk membentuk Gen Z menjadi individu yang mampu berinteraksi secara aman dan cerdas di dunia digital.

Daftar Pustaka.

- Mackness MI, Mackness B, Durrington PN, Fogelman AM, Berliner J and Lusic AJ. 2017. Paraoxonase and coronary heart disease. *Curr. Opin. Lipidol.* 9: 319-24.
- Cyber Security Agency. (2022). National Cyber Security Awareness Survey. [URL jika ada]
- Kaspersky. (2023). AI in Cybersecurity: Trends and Threats. [URL jika ada]
- Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's internet use. *Journal of Broadcasting & Electronic Media*, 52(4), 581-599.
- OECD. (2021). *The Digital Transformation of Education: Challenges and Opportunities*. OECD Publishing.
- Syahrul, S. (2022). Students' motivation In Learning English By Giving Warm Up Activities In Beginning Of Class. *Exposure: Jurnal Pendidikan Bahasa Inggris*, 11(2), 214-236.
- Hermawan, H., Ibumal, I., & Syahrul, S. (2024). COOPERATIVE LEARNING IN TEACHING READING: How does the English teacher perceive cooperative learning?. *EXPOSURE: JURNAL PENDIDIKAN BAHASA INGGRIS*, 13(2), 693-703.
- Syahrul, S., & Hamzah, M. Q. (2024). PENGGUNAAN BAHASA INGGRIS PADA KARYAWAN BANK SYARIAH: Analisis Penggunaan Bahasa Inggris pada Karyawan Bank Syariah Di Kota Makassar. *Journal of Institution and Sharia Finance*, 7(2), 52-63.
- Pew Research Center. (2019). *Gen Z Looks to the Future*.
- Smith, J., & Jones, A. (2020). Digital Footprint and Privacy Perceptions Among Gen Z in Emerging Economies. [Nama Jurnal/Prosiding jika fiktif, atau "Unpublished Manuscript"].
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151.