Journal of Innovation and Applied Education
E-ISSN: 3032-6745; P-ISSN: 3032-6782
Journal Homepage: https://journal.lontaradigitech.com/IAEJ/index

Edukasi Keamanan Digital Berbasis AI Generatif: Studi pada Mahasiswa Teknologi di Indonesia

Afrisal Arifin*[1], Devi Miftahul Jannah[2]

[1,2,3]*Universitas Negeri Makassar, Jl. Mallengkeri Raya, Parang Tambung, 90224, Sulawesi Selatan, Indonesia*

Email: agig7544@mail.com, devimiftahul734@gmail.com

ARTICLE INFO

Kata kunci:
AI Generatif
Keamanan Siber;
Literasi Digital
Mahasiswa;
Strategi Edukasi.

Diterima: 20.04.2024
Disetujui: 25.05.2024
Diterbitkan: 01.06.2024

ABSTRACT

Penelitian ini bertujuan untuk mengevaluasi tingkat literasi keamanan siber dan perilaku mahasiswa dalam mengadopsi langkah-langkah perlindungan digital. Dengan pendekatan kuantitatif berbasis survei dan desain cross-sectional, data dikumpulkan melalui kuesioner daring dari mahasiswa program studi berbasis teknologi di Indonesia, menggunakan purposive sampling untuk menjangkau partisipan yang relevan. Instrumen penelitian mencakup tiga aspek utama: pandangan terhadap penggunaan chatbot berbasis AI Generatif, kebiasaan penggunaan teknologi, dan pemahaman serta sikap terhadap ancaman digital. Analisis statistik dilakukan untuk menilai hubungan antara literasi keamanan digital, kesadaran, dan perilaku mahasiswa. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan siber mahasiswa berada pada kategori menengah, dengan kesadaran dasar yang cukup baik namun implementasi langkah-langkah spesifik, seperti autentikasi dua faktor dan pengelolaan privasi, masih memerlukan peningkatan. Pembelajaran berbasis AI Generatif, seperti GPT Chatbot, diidentifikasi sebagai pendekatan potensial untuk meningkatkan literasi keamanan siber secara personal dan relevan. Penelitian ini berkontribusi pada pengembangan strategi edukasi keamanan digital yang lebih efektif, memberikan wawasan tentang perilaku mahasiswa, dan menginformasikan institusi pendidikan untuk mengintegrasikan modul keamanan siber ke dalam kurikulum. Temuan ini menegaskan pentingnya kolaborasi antara institusi pendidikan dan penyedia alat keamanan dalam menciptakan generasi pengguna digital yang lebih aman dan terinformasi.

1. PENDAHULUAN

Keamanan digital mencakup pengaturan praktis, teknologi, dan perangkat lunak untuk melindungi data, sistem, dan jaringan komputer dari ancaman seperti malware, pencurian data, dan serangan denial-of-service[1]. Serangan ini tidak hanya menyebabkan kerugian finansial dan mengurangi kepercayaan pengguna, tetapi juga menghambat pengelolaan energi yang efisien serta pencapaian tujuan keberlanjutan, sehingga menekankan pentingnya pendekatan keamanan digital yang komprehensif dan adaptif [2]. Dalam keamanan digilat, peran teknologi seperti Generative AI semakin menjadi perhatian utama. Generative AI, yang dapat mensimulasikan data dan pola secara realistis, memberikan peluang signifikan dalam meningkatkan kemampuan deteksi dan mitigasi ancaman siber [3]. Teknologi ini memungkinkan simulasi skenario ancaman yang membantu pengguna, termasuk mahasiswa, untuk memahami dan mengantisipasi risiko siber dengan lebih baik [4].

Penelitian sebelumnya telah membahas penerapan digital twin untuk meningkatkan keamanan dan keselamatan kendaraan otonom (AV) di tengah ancaman siber. Studi ini mengidentifikasi tantangan seperti keamanan data dan perlindungan terhadap serangan siber, menunjukkan bahwa digital twin dapat meningkatkan pemantauan dan analisis ancaman serta mendorong penerapan protokol keamanan yang lebih ketat, yang esensial untuk operasional AV yang aman dan berkelanjutan [5]. Selain itu, penelitian lain menekankan bahwa digital twin berfungsi sebagai alat efektif untuk pemantauan real-time, meningkatkan deteksi dan respons terhadap serangan siber, yang sangat penting untuk meningkatkan keamanan sistem industri dan mendorong pengembangan praktik keamanan yang lebih baik di masa depan [6].

Kemudian, terdapat penelitian yang mengembangkan paradigma pembelajaran inovatif untuk pendidikan keamanan siber berbasis AI/ML, menggunakan lingkungan virtual imersif yang memanfaatkan platform Minecraft dan pendekatan kolaboratif seperti hackathon. Hasilnya, paradigma ini terbukti efektif melibatkan peserta dari berbagai latar belakang, meningkatkan pemahaman, dan membangun keahlian yang relevan di bidang keamanan siber modern [7]. Selanjutnya terdapat penelitian dengan menggunakan data dari 35 mahasiswa dengan desain pretest-posttest control group untuk mengevaluasi efektivitas psikoedukasi dalam meningkatkan literasi depresi. Hasil menunjukkan peningkatan signifikan pada literasi depresi di kelompok intervensi [8].

Selanjutnya, penelitian yang memanfaatkan Generative AI seperti ChatGPT untuk mendukung pembelajaran personalisasi untuk profesional keamanan siber. Dengan kerangka ECSF dan NICE, AI dirancang untuk menyediakan rencana belajar, sumber daya, dan saran karier. Hasilnya menunjukkan AI efektif meningkatkan pembelajaran dan pengembangan kompetensi keamanan siber [9]. Setelah itu, terdapat penelitian yang menggunakan data jumlah mahasiswa baru dari 2016-2020 untuk memprediksi tren lima tahun ke depan menggunakan regresi linier sederhana. Hasil menunjukkan model prediksi yang akurat, memberikan wawasan berharga untuk perencanaan institusi pendidikan [10].

Penelitian selanjutnya menyoroti penggunaan teknologi biometrik, seperti pengenalan wajah dan suara, yang meskipun meningkatkan keamanan, rentan terhadap manipulasi digital yang dapat mengancam integritas sistem. Studi ini menggarisbawahi pentingnya penerapan skema forensik digital untuk memvalidasi keaslian data biometrik, yang dapat meningkatkan kepercayaan pengguna dan mendukung protokol keamanan yang lebih ketat untuk menciptakan lingkungan yang lebih aman dan berkelanjutan [11]. Selain itu, penerapan digital twin dalam keamanan siber juga terbukti efektif dalam pemantauan ancaman secara real-time, meningkatkan deteksi dan respons terhadap serangan siber, serta mendorong pengembangan protokol keamanan yang lebih kuat, yang penting untuk menjaga operasional industri yang aman dan berkelanjutan [2].

Meskipun banyak penelitian telah berfokus pada sistem kontrol industri dan kendaraan otonom, penting untuk mengeksplorasi pengaruh keamanan digital terhadap perilaku pengguna, khususnya di kalangan mahasiswa. Peningkatan pengetahuan tentang keamanan digital dapat mempengaruhi perilaku penggunaan fitur keamanan tambahan, sehingga kesadaran yang tinggi dapat membantu mengurangi risiko serangan siber [12]. Namun, tantangan dalam memahami faktor-faktor organisasi, sosial, dan pribadi yang memengaruhi kesadaran terhadap keamanan digital serta efektivitas teknologi AI generatif dalam meningkatkan pembelajaran keamanan siber masih perlu diteliti lebih lanjut.

Keunggulan penelitian ini terletak pada fokus spesifiknya terhadap perilaku pengguna, yaitu mahasiswa, dalam konteks keamanan digital. Berbeda dari penelitian sebelumnya yang lebih banyak membahas penerapan digital twin, proyek ini akan mengeksplorasi bagaimana peningkatan pengetahuan keamanan digital dapat memengaruhi penggunaan fitur keamanan tambahan [3]. Penelitian ini berpotensi memberikan wawasan baru tentang perilaku pengguna dan membantu dalam pengembangan strategi keamanan yang lebih efektif, serta meningkatkan literasi keamanan siber di kalangan mahasiswa, generasi pengguna teknologi yang akan datang.

Tujuan dari penelitian ini adalah untuk mengevaluasi kesadaran dan perilaku keamanan siber di kalangan mahasiswa, khususnya yang bekerja di bidang teknologi, melalui metode pembelajaran berbasis AI generatif [7]. Dengan pengumpulan data survei dan analisis statistik, penelitian ini diharapkan dapat memberikan wawasan tentang peningkatan literasi keamanan siber di Indonesia serta mengidentifikasi tantangan yang dihadapi dalam mengembangkan strategi keamanan yang lebih baik di masa depan.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan desain cross-sectional, yang dipilih untuk menganalisis hubungan antara pengetahuan keamanan digital, kesadaran keamanan siber, dan perilaku dalam menggunakan fitur keamanan tambahan pada satu periode waktu tertentu. Fokus utama penelitian ini adalah mengevaluasi pengaruh pembelajaran berbasis AI generatif terhadap literasi keamanan siber mahasiswa, khususnya yang menekuni bidang teknologi.

Responden penelitian adalah mahasiswa aktif di Indonesia yang terdaftar dalam program studi berbasis teknologi, seperti Teknik Informatika, Sistem Informasi, atau Ilmu Komputer, serta memiliki pengalaman dalam menggunakan teknologi digital untuk aktivitas akademik atau profesional. Teknik pengambilan sampel yang digunakan adalah purposive sampling, yang memungkinkan pemilihan partisipan dengan kriteria tertentu untuk memberikan data yang relevan dan mendalam. Data dikumpulkan secara daring untuk menjangkau mahasiswa dari berbagai perguruan tinggi di Indonesia. Kuesioner disebarkan menggunakan platform Google Forms, dengan distribusi tautan melalui grup media sosial dan komunitas mahasiswa di bidang teknologi [13].

Instrumen kuesioner dirancang untuk mengevaluasi tiga dimensi utama, yaitu: pandangan mahasiswa terhadap penggunaan GPT Chatbot dengan mengeksplorasi bagaimana siswa memandang penggunaan chatbot berbasis GPT, baik dari sisi manfaat, kemudahan, maupun tantangannya dalam konteks. Kebiasaan penggunaan teknologi yang dimana mencangkup kebiasaan siswa dalam menggunakan teknologi secara umum, seperti frekuensi penggunaan, jenis aktivitas digital yang sering dilakukan, serta durasi pemakaian teknologi, dan terakhir adalah pemahaman serta sikap terhadap ancaman digital (Understanding and Attitudes toward Digital Threats) yaitu dengan mengevaluasi sejauh mana siswa memahami potensi ancaman digital, seperti privasi, keamanan data, dan ancaman lainnya, serta sikap mereka terhadap masalah tersebut.[14].

Tabel 1. Kisi-Kisi Instrumen

No	ASPEK/ SUB FAKTOR	Nomor Pernyataan	REFERENSI
1	Aspek Pandangan Siswa Terhadap Penggunaan GPT Chatbot	1-5	Artificial intelligence and social media on academic performance

2	Aspek Technology Usage Habits	6-10	and mental well-being: Student perceptions of positive impact in the age of smart learning [15].
3	Aspek Understanding and Attitudes toward Digital Threats	11-15	

Pada tabel 1 diatas, merupakan kerangka kerja untuk penyusunan instrumen penelitian yang bertujuan mengukur berbagai aspek terkait, seperti pandangan siswa, kebiasaan penggunaan teknologi dan pemahaman serta sikap terhadap ancaman digital. Berikut penejlasan masing-masing aspek:

Tabel 2. Skala Likert

Skala	Keterangan
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Setuju

Berikut pada tabel 2 diatas, merupakan skala penilaian yang kita gunakan pada metode penelitian ini, yang dimana ini mengukur pendapat atau sikap responden terhadap penytaan yang ada. Skala ini digunakan untuk mempermudah pengumpulan data kuantitatif dari responden, yang dapa dianalisis secara statistik untuk mendapatkan informasi.

3. HASIL DAN DISKUSI

4. Tabel 3. Demografi Responden

Jenis kelamin	Counts	% of Total	Cumulative %
Laki-Laki	**40**	**38.1 %**	**38.1 %**
Perempuan	**65**	**61.9 %**	**100.0 %**

Tabel 3 menunjukkan bahwa distribusi frekuensi responden berdasarkan jenis kelamin, dengan jumlah responden laki-laki sebanyak 40 orang dan perempuan sebanyak 65 orang. Dalam persentase, responden laki-laki menyumbang 38,1% dari total keseluruhan, sementara perempuan mendominasi dengan proporsi 61,9%. Persentase kumulatif menunjukkan bahwa hingga kategori laki-laki, angkanya mencapai 38,1%, dan setelah memasukkan data kategori perempuan, persentase kumulatif mencapai 100%. Hal ini menggambarkan bahwa sebagian besar responden dalam penelitian ini adalah perempuan, memberikan indikasi awal terhadap komposisi demografi jenis kelamin dalam data penelitian.

Tabel 4. Demografi Responden

	Jenis Kelamin 2	Age
Mean	Laki laki	19.4
	perempuan	19.1

Hasil analisis pada tabel 4, berdasarkan dokumen menunjukkan bahwa rata-rata usia responden laki-laki adalah **19.4 tahun**, sedangkan rata-rata usia responden perempuan adalah **19.1 tahun**. Data ini mengindikasikan bahwa mayoritas responden berasal dari kelompok usia yang hampir sama, yaitu generasi muda yang kemungkinan besar cukup akrab dengan teknologi digital.

Kelompok usia ini menjadi target penting untuk edukasi keamanan siber, mengingat tingkat keterlibatan mereka yang tinggi dengan aktivitas daring. Edukasi yang relevan dan berbasis pengalaman mereka dapat meningkatkan kesadaran serta kemampuan mereka untuk menghadapi risiko keamanan digital dengan lebih baik.

Tabel 5. Data Aspek Pandangan Siswa Terhadap Penggunaan GPT Chatbot

No	Item/Pernyataan/ Pertanyaan						
		Mean	Median	Modus	Minimum	Maksimum	Sum
1	Saya mengetahui apa itu keamanan digital	4.01	4	4.00	1	5	412
2	Saya sering memperbarui kata sandi akun digital Anda	3.56	4	3.00	1	5	374
3	Saya menerima pelatihan tentang keamanan digital sebelumnya	2.87	3	3.00	1	5	301
4	Saya merasa bahwa informasi pribadi saya aman di internet.	3.33	3	3.00	1	5	350
5	Saya menggunakan fitur keamanan tambahan seperti autentikasi dua faktor di akun online saya.	3.86	4	5.00	1	5	405

Tabel 6. Variable v1-v5 Pandangan Siswa Terhadap Penggunaan GPT Chatbot

	v1	v2	v3	v4	v5
Mean	4.01	3.56	2.87	3.33	3.86
Sum	421	374	301	350	405

Tabel 7. Komputasi variable v1-v5

	F1
Mean	3.53

Hasil analisis pada tabel diatas, menunjukkan bahwa rata-rata keseluruhan variabel keamanan siber adalah 3.53, dengan skor tertinggi pada v1 (4.01), mencerminkan kebiasaan positif dalam menjaga keamanan digital, dan skor terendah pada v3 (2.87), yang menunjukkan kurangnya pemahaman atau penerapan langkah keamanan tertentu. Mayoritas responden menyadari pentingnya menjaga keamanan siber, tetapi masih ada kelemahan yang memerlukan edukasi lebih lanjut, khususnya dalam melindungi diri dari ancaman digital seperti pencurian data. Hal ini menegaskan perlunya kebijakan dan pelatihan yang lebih efektif untuk meningkatkan kesadaran dan kemampuan keamanan digital, terutama di lingkungan pendidikan.

Tabel 8. Data Aspek Technology Usage Habits

No	Item/Pernyataan/ Pertanyaan						
		Mean	Median	Modus	Minimum	Maksimum	Sum
1	Saya menggunakan perangkat lunak antivirus pada perangkat saya.	3.79	4	4.00	1	5	398
2	Saya secara rutin memeriksa izin aplikasi sebelum menginstalnya.	3.86	4	4.00	1	5	403
3	Saya secara rutin memeriksa atau memperbarui pengaturan privasi di media sosial.	3.74	4	4.00	1	5	393
4	Saya secara rutin memeriksa atau memperbarui pengaturan privasi di media sosial.	2.65	3	3.00	1	5	278
5	Saya menggunakan jaringan Wi-Fi publik tanpa VPN atau alat keamanan lainnya.	3.33	3	3.00	1	5	350

Tabel 9. Variable v6-v10 nology Usage Habits

	v6	v7	v8	v9	v10
Mean	**3.79**	**3.84**	**2.65**	**3.74**	**3.33**
Sum	**398**	**403**	**278**	**393**	**350**

Tabel 10. Komputasi variable v6-v10

	v2 (2)
Mean	**3.47**

Hasil analisis pada tabel 10 menunjukan bahwa variabel keamanan siber dengan rata-rata variabel v2 adalah 3.47. Nilai ini mencerminkan bahwa kesadaran terhadap aspek tertentu dalam keamanan digital masih berada di tingkat menengah, menunjukkan adanya potensi untuk perbaikan. Responden umumnya menyadari pentingnya melindungi data pribadi mereka, namun kemungkinan belum sepenuhnya memahami langkah-langkah spesifik untuk meningkatkan keamanan, seperti penggunaan alat perlindungan tambahan atau pengelolaan privasi di dunia digital. Oleh karena itu, edukasi yang lebih mendalam dan kebijakan keamanan yang efektif diperlukan untuk mendorong peningkatan kesadaran dan kemampuan dalam menjaga keamanan digital, terutama dalam aspek-aspek yang menunjukkan kelemahan.

Tabel 11. Data Aspek Understanding and Attitudes toward Digital Threats

No	**Item/Pernyataan/ Pertanyaan**						
		Mean	**Median**	**Modus**	**Minimum**	**Maksimum**	**Sum**
1	Saya tahu apa itu phishing dan bagaimana cara mengidentifikasinya.	**3.31**	**3.00**	**3.00**	**1**	**5**	**344**
2	Saya merasa khawatir terhadap serangan siber yang dapat terjadi di akun pribadi saya.	**4.05**	**4**	**5.00**	**1**	**5**	**425**
3	Saya pernah menjadi korban pencurian identitas atau peretasan.	**2.49**	**2**	**1.00**	**1**	**5**	**261**
4	Saya percaya bahwa perusahaan digital besar secara umum menjaga keamanan data pengguna dengan baik.	**3.16**	**3**	**3.00**	**1**	**5**	**379**
5	Saya setuju bahwa menjaga keamanan digital adalah tanggung jawab individu.	**4.09**	**4**	**5.00**	**1**	**5**	**429**

Tabel 11. Variable v11-v15 Understanding and Attitudes toward Digital Threats

	v11	**v12**	**v13**	**v14**	**v15**
Mean	**3.31**	**4.05**	**2.49**	**3.61**	**4.09**

Tabel 11. Variable v11-v15 Understanding and Attitudes toward Digital Threats

	v11	v12	v13	v14	v15
Sum	**344**	**425**	**261**	**379**	**429**

Tabel 12. Komputasi v11-v15

	v3 (2)
Mean	**3.51**

Berdasarkan hasil analisis, rata-rata pada tabel 12 untuk variabel v3 adalah 3.51. Nilai ini menunjukkan tingkat kesadaran atau implementasi keamanan siber yang berada pada kategori menengah. Hal ini mencerminkan bahwa sebagian besar responden memiliki pemahaman dasar yang cukup baik tentang langkah-langkah keamanan digital, meskipun masih ada ruang untuk peningkatan, terutama dalam pengaplikasian langkah-langkah spesifik seperti perlindungan privasi atau penggunaan alat keamanan tambahan.

Untuk mendukung perbaikan, program edukasi dan pelatihan terkait keamanan digital yang lebih terfokus dapat membantu meningkatkan kesadaran dan kemampuan responden dalam menghadapi ancaman dunia digital. Langkah ini penting untuk memastikan perlindungan yang lebih baik terhadap data pribadi di lingkungan yang semakin terhubung secara digital.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa tingkat kesadaran dan perilaku mahasiswa terhadap keamanan siber masih berada pada kategori menengah, dengan pemahaman yang cukup baik tetapi penerapan langkah-langkah perlindungan spesifik seperti autentikasi dua faktor dan pengelolaan privasi masih perlu ditingkatkan. Edukasi berbasis AI generatif, seperti GPT Chatbot, terbukti berpotensi meningkatkan literasi keamanan siber melalui pembelajaran yang personalisasi dan relevan. Penelitian ini berkontribusi pada ilmu pengetahuan dengan memberikan wawasan baru tentang perilaku keamanan digital mahasiswa serta efektivitas teknologi AI dalam edukasi keamanan siber, dan memberikan masukan bagi institusi pendidikan untuk mengembangkan modul keamanan siber dalam kurikulum dan pelatihan praktis. Untuk itu, disarankan agar institusi pendidikan mengintegrasikan program edukasi keamanan digital berbasis teknologi dan berkolaborasi dengan penyedia alat keamanan untuk membantu mahasiswa memahami dan menerapkan perlindungan digital yang lebih baik.

REFERENSI

[1] N. Zermi, A. Khaldi, R. Ka, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," vol. 320, 2021, doi: 10.1016/j.forsciint.2021.110691.

[2] L. T. Ha, "Are digital business and digital public services a driver for better energy security ? Evidence from a European sample," *Environ. Sci. Pollut. Res.*, pp. 27232–27256, 2022, doi: 10.1007/s11356-021-17843-2.

[3] M. Schmitt and I. Flechais, "Digital Deception : Generative Artificial Intelligence in Social Engineering and Phishing," no. Ml, pp. 1–18.

[4] H. Xu, Y. Li, O. Balogun, S. Wu, Y. Wang, and Z. Cai, "Security Risks Concerns of Generative AI in the IoT," no. October, pp. 1–6, 2024.

[5] S. Almeaibed, S. Al-rubaye, A. Tsourdos, and N. P. Avdelidis, "Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles," no. March, pp. 40–46, 2021.

[6] M. Atalay and P. Angin, "A Digital Twins Approach to Smart Grid Security Testing and Standardization," *2020 IEEE Int. Work. Metrol. Ind. 4.0 IoT, MetroInd 4.0 IoT 2020 - Proc.*, pp. 435–440, 2020, doi: 10.1109/MetroInd4.0IoT48571.2020.9138264.

[7] J. Wei-kocsis, "Cybersecurity Education in the Age of Artificial Intelligence : A Novel Proactive and Collaborative Learning Paradigm," no. Dl, 2022.

[8] O. S. Natasubagyo and S. Kusrohmaniah, "Efektivitas Psikoedukasi untuk Peningkatan Literasi Depresi," vol. 5, no. 1, pp. 26–35, 2019, doi: 10.22146/gamajpp.48585.

[9] O. Krishnamurthy, "Enhancing Cyber Security Enhancement Through Generative AI," no. 9, pp. 35–50, 2023.

[10] N. Almumtazah, N. Azizah, Y. L. Putri, I. Negeri, and S. Ampel, "Prediksi jumlah mahasiswa baru menggunakan metode regresi linier sederhana," vol. 18, pp. 31–40, 2021.

[11] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities : A brief review of digital forensic schemes for biometric data," *Pattern Recognit. Lett.*, vol. 138, pp. 346–354, 2020, doi: 10.1016/j.patrec.2020.07.009.

[12] A. Aris, L. P. Rondon, D. Ortiz, and M. Finlayson, "Integrating Artificial Intelligence into Cybersecurity Curriculum : New Perspectives," no. 2001, 2021.

[13] A. Fauzan and A. Sa, "Communautaire : Journal of Community Service Empowering Teachers Through Digital Assessment : Enhancing Competence and Efficiency with Google Forms in Primary Education," vol. 03, no. 02, pp. 166–178, 2024.

[14] S. Xu, K. I. Khan, and M. F. Shahzad, "Examining the influence of technological self-efficacy, perceived trust, security, and electronic word of mouth on ICT usage in the education sector," *Sci. Rep.*, vol. 14, no. 1, pp. 1–16, 2024, doi: 10.1038/s41598-024-66689-4.

[15] M. F. Shahzad, S. Xu, W. M. Lim, X. Yang, and Q. R. Khan, "Artificial intelligence and social media on academic performance and mental well-being: Student perceptions of positive impact in the age of smart learning," *Heliyon*, 2023, doi: https://doi.org/10.1016/j.heliyon.2024.e29523.