Sosialisasi Bahaya Phishing dan Tips Aman Menggunakan Internet bagi Mahasiswa

Sutarman[a], Ade May Luky Harefa[b]
[a]Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sumatera Utara, Medan, 20155, Indonesia
[b]Magister Teknologi Informasi, Universitas Pembangunan Panca Budi, Medan, 20122, Indonesia
Penulis Koresponden: (e-mail: sutarman@usu.ac.id), ademayluky@gmail.com,

ABSTRAK Kegiatan pengabdian kepada masyarakat ini dilaksanakan dengan tujuan untuk meningkatkan literasi keamanan digital mahasiswa, khususnya dalam memahami dan mengantisipasi serangan phishing. Sasaran kegiatan ini adalah mahasiswa Ilmu Komputer Semester 4 di Institut Bisnis dan Komputer Indonesia. Berdasarkan hasil observasi awal, ditemukan bahwa masih banyak mahasiswa yang belum memahami ciri-ciri umum phishing, seperti tautan mencurigakan, email palsu, hingga situs web tiruan. Kegiatan ini dilaksanakan melalui metode sosialisasi berbasis teori, simulasi kasus nyata, serta diskusi interaktif. Evaluasi dilakukan menggunakan pre-test dan post-test dengan soal yang sama untuk mengukur peningkatan pemahaman peserta. Hasil pre-test menunjukkan bahwa 70% peserta belum memahami bentuk phishing secara mendalam. Namun, setelah kegiatan berlangsung, hasil post-test menunjukkan peningkatan signifikan, di mana 90% peserta berhasil menjawab minimal 8 dari 10 soal dengan benar. Peserta juga menunjukkan perubahan sikap, lebih waspada dalam menggunakan internet dan mampu mengidentifikasi ancaman phishing secara mandiri. Metode penyampaian yang interaktif terbukti efektif dalam meningkatkan pemahaman peserta. Kegiatan ini dinilai sangat bermanfaat dan direkomendasikan untuk terus dilanjutkan dengan cakupan audiens yang lebih luas, guna menciptakan lingkungan digital yang aman dan sadar akan ancaman siber.

KATA KUNCI *Keamanan Informasi, Literasi Digital, Phishing, Sosialisasi Edukatif.*

1. PENGANTAR

Perkembangan teknologi informasi dan komunikasi telah membawa dampak yang sangat besar dalam kehidupan manusia, termasuk dalam dunia pendidikan tinggi (Huraerah dkk., 2024). Mahasiswa sebagai bagian dari generasi digital native setiap hari berinteraksi dengan berbagai bentuk layanan digital seperti email, media sosial, layanan cloud, serta berbagai platform perkuliahan daring (Purba, 2023). Keterampilan menggunakan teknologi menjadi bagian tak terpisahkan dalam proses belajar dan kehidupan akademik (Surya dan Moramowati, 2023). Namun di balik kemudahan tersebut, terdapat ancaman serius yang seringkali luput dari perhatian mahasiswa, salah satunya adalah kejahatan siber dalam bentuk phishing.

Phishing merupakan metode penipuan yang dilakukan oleh pihak tidak bertanggung jawab untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan data kartu kredit, dengan cara menyamar sebagai entitas terpercaya dalam komunikasi digital (Dharani dkk., 2024). Phishing seringkali muncul dalam bentuk email palsu, pesan teks, atau tautan yang mengarahkan korban ke situs palsu yang menyerupai situs resmi (Kainde dkk., 2024). Meski telah banyak kampanye literasi digital, kenyataannya masih banyak mahasiswa yang belum memiliki pemahaman yang cukup mengenai cara kerja phishing dan cara menghindarinya. Hal ini menimbulkan kerentanan yang dapat berdampak pada keamanan data pribadi bahkan kerugian finansial.

Melihat fenomena tersebut, diperlukan upaya edukatif yang sistematis dalam bentuk sosialisasi dan pelatihan mengenai bahaya phishing dan pentingnya menjaga keamanan dalam penggunaan internet. Kegiatan pengabdian kepada masyarakat ini merupakan salah satu bentuk kontribusi nyata sivitas akademika, khususnya mahasiswa dan dosen program studi Ilmu Komputer, dalam meningkatkan kesadaran akan pentingnya keamanan digital di lingkungan kampus. Mahasiswa tidak hanya dituntut cakap dalam menggunakan teknologi, tetapi juga cerdas dan bijak dalam melindungi identitas digital mereka.

Tujuan utama dari kegiatan ini adalah untuk memberikan pemahaman mendalam kepada mahasiswa mengenai jenis-jenis phishing, cara kerja serangan ini, serta langkah-langkah pencegahan yang dapat dilakukan. Selain itu, kegiatan ini juga bertujuan untuk membentuk sikap kritis terhadap konten digital yang mencurigakan, serta mendorong mahasiswa untuk menerapkan kebiasaan aman dalam menggunakan internet. Materi yang disampaikan akan mencakup contoh-contoh kasus nyata, pemaparan teknik pengamanan dasar, serta praktik langsung mengenali email atau situs phishing.

Kegiatan ini ditujukan kepada mahasiswa Ilmu Komputer semester 4 di Institut Bisnis dan Komputer Indonesia, yang dianggap telah memiliki dasar penggunaan teknologi namun belum sepenuhnya memahami risiko keamanan digital. Melalui pendekatan interaktif seperti presentasi, diskusi kelompok, dan simulasi kasus, diharapkan para peserta dapat terlibat aktif dan memperoleh wawasan yang aplikatif. Capaian dari kegiatan ini diukur dari peningkatan pemahaman peserta yang dievaluasi melalui pre-test dan post-test, serta tindak lanjut dalam bentuk poster edukasi yang disebarluaskan di lingkungan kampus.

Kegiatan ini dirancang sebagai pelaksanaan satu kali, namun dengan kemungkinan berkelanjutan jika terdapat kebutuhan lanjutan dari mahasiswa atau pihak institusi. Apabila kegiatan ini berhasil mencapai target dan mendapat respon positif dari peserta, maka akan dipertimbangkan untuk dijadikan program tahunan atau dikembangkan menjadi modul pembelajaran keamanan digital bagi seluruh mahasiswa di berbagai jenjang. Dengan demikian, kegiatan pengabdian ini tidak hanya berdampak sesaat, tetapi juga memberikan kontribusi jangka panjang terhadap peningkatan literasi keamanan digital di kalangan mahasiswa.

2. STUDI KEPUSTAKAAN

Penggunaan internet secara masif dalam kehidupan sehari-hari telah mengubah pola interaksi sosial, cara belajar, serta metode penyampaian informasi di lingkungan pendidikan tinggi (Situmorang, 2023). Berdasarkan data dari *We Are Social dan Hootsuite*, pengguna internet di Indonesia telah mencapai lebih dari 213 juta orang, dengan mayoritas pengguna berasal dari kalangan usia produktif, termasuk mahasiswa (Ratutara dan Yusuf, 2025). Kondisi ini menunjukkan betapa tingginya ketergantungan masyarakat terhadap teknologi informasi dan komunikasi (TIK), termasuk dalam aktivitas akademik di perguruan tinggi.

Meskipun mahasiswa dianggap sebagai digital native, banyak dari mereka yang masih memiliki pemahaman terbatas terkait dengan ancaman keamanan siber, terutama serangan phishing. Menurut Verizon Data Breach Investigations Report (2023), phishing masih menjadi metode paling umum dalam upaya pencurian data digital, yang mencakup lebih dari 36% dari seluruh serangan siber global. Phishing sangat efektif karena mengeksploitasi ketidaktahuan atau kelalaian pengguna terhadap pesan atau situs palsu yang menyerupai entitas resmi.

Menurut (Budiono dkk., 2025), phishing dapat dilakukan melalui berbagai saluran seperti email, pesan instan, bahkan media sosial. Ciri-ciri umum dari serangan phishing antara lain pesan yang mendesak, tautan yang tidak dikenal, dan permintaan informasi sensitif (Kainde dkk., 2024). Pengguna yang tidak memiliki kesadaran dan keterampilan dasar keamanan digital akan dengan mudah menjadi korban. Oleh karena itu, penting untuk memberikan edukasi mengenai cara mengenali dan mencegah phishing, terutama kepada kelompok yang aktif menggunakan internet dalam aktivitas sehari-hari seperti mahasiswa.

Dalam konteks pendidikan tinggi, literasi digital bukan hanya terbatas pada kemampuan mengoperasikan perangkat atau aplikasi, tetapi juga mencakup aspek keselamatan digital (digital safety). Menurut (Budiono dkk., 2025), literasi digital yang kuat mampu meningkatkan kesadaran kritis terhadap risiko online dan membantu pengguna mengembangkan strategi perlindungan diri. Dengan membekali mahasiswa dengan keterampilan ini, institusi pendidikan turut berperan dalam menciptakan lingkungan belajar yang aman secara digital.

Beberapa penelitian terdahulu juga menegaskan urgensi edukasi mengenai keamanan digital. Studi (Samsumar dkk., 2025) menyebutkan bahwa mahasiswa seringkali mengabaikan protokol keamanan seperti penggunaan autentikasi dua faktor atau verifikasi sumber tautan, padahal hal ini penting untuk mencegah pencurian akun dan data. Demikian pula, (Aska dkk., 2024) dalam penelitiannya menunjukkan bahwa pelatihan keamanan siber berbasis simulasi memiliki efektivitas tinggi dalam meningkatkan pemahaman mahasiswa tentang phishing.

Berdasarkan kajian tersebut, dapat disimpulkan bahwa pemahaman mahasiswa terhadap phishing masih perlu ditingkatkan melalui pendekatan edukatif yang sistematis. Kegiatan sosialisasi ini dirancang untuk menjawab kebutuhan tersebut, dengan menyasar mahasiswa Ilmu Komputer yang diharapkan tidak hanya menjadi pengguna teknologi, tetapi juga agen perubahan dalam menyebarkan praktik keamanan digital yang baik di lingkungan kampus maupun masyarakat.

3. METODOLOGI

Kegiatan pengabdian kepada masyarakat ini dilaksanakan dengan menggunakan metode sosialisasi dan pelatihan interaktif yang dirancang secara sistematis untuk meningkatkan pemahaman mahasiswa mengenai bahaya phishing dan praktik keamanan digital yang tepat. Pendekatan yang digunakan bersifat edukatif, partisipatif, dan aplikatif, agar materi yang disampaikan mudah diterima serta dapat langsung diterapkan oleh peserta dalam kehidupan sehari-hari.

Sebelum pelaksanaan kegiatan, dilakukan analisis kebutuhan (need assessment) melalui diskusi informal dengan beberapa mahasiswa dan dosen program studi Ilmu Komputer untuk mengetahui sejauh mana pemahaman mereka terhadap isu phishing dan keamanan digital. Hasil dari diskusi ini menunjukkan bahwa sebagian besar mahasiswa belum memiliki pengetahuan yang memadai tentang teknik phishing serta cara menghindarinya. Berdasarkan temuan tersebut, tim pengabdian menyusun materi dan metode yang sesuai dengan tingkat pemahaman mahasiswa.

Metode pelaksanaan kegiatan terdiri atas beberapa tahapan, yaitu:

Jurnal Pengabdian Kepada Masyarakat
Teknologi Informasi dan Komunikasi (PKM-TIK)
E-ISSN :3090-1588 (Online)

a. Persiapan: meliputi penyusunan modul sosialisasi, pembuatan media presentasi (slide dan video), serta penyusunan pre-test dan post-test untuk mengukur tingkat pemahaman peserta.
b. Pelaksanaan Sosialisasi: kegiatan dilaksanakan secara luring (offline) di ruang kelas kampus dengan metode ceramah, diskusi interaktif, dan studi kasus. Narasumber menjelaskan konsep phishing, contoh-contoh kasus nyata, serta tips menghindari jebakan phishing.
c. Simulasi dan Praktik: peserta diberikan contoh email atau tautan palsu, lalu diajak untuk mengidentifikasi ciri-ciri phishing secara langsung. Tujuannya agar mahasiswa terbiasa bersikap kritis terhadap informasi digital yang diterima.
d. Evaluasi: dilakukan pre-test sebelum kegiatan dan post-test setelah kegiatan untuk mengukur efektivitas penyampaian materi. Selain itu, peserta diminta memberikan umpan balik (feedback) melalui kuesioner singkat.

Kegiatan ini juga menghasilkan luaran dalam bentuk media edukasi seperti poster digital berisi tips keamanan digital dan infografis mengenai phishing, yang disebarkan melalui media sosial kampus untuk menjangkau mahasiswa yang tidak ikut langsung dalam kegiatan. Sebagai bentuk keberlanjutan, tim pengabdian juga menyusun pedoman singkat (leaflet) yang dapat digunakan secara mandiri oleh mahasiswa sebagai panduan mengenali phishing. Dengan metodologi ini, diharapkan terjadi peningkatan literasi keamanan digital pada mahasiswa Ilmu Komputer, serta tercipta lingkungan kampus yang lebih aman dari ancaman kejahatan siber. Pendekatan interaktif dan berbasis simulasi yang diterapkan juga menjadi kebaruan dalam bentuk edukasi praktis yang relevan dengan tantangan dunia digital saat ini.

4. HASIL DAN PELAKSANAAN

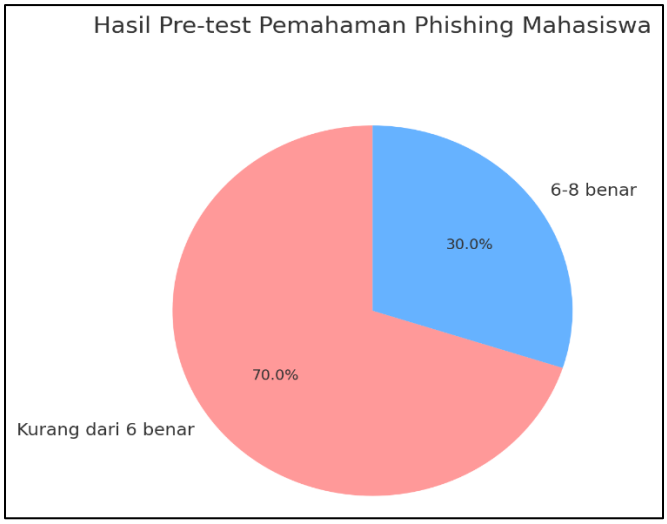
Kegiatan pengabdian kepada masyarakat berjudul “Sosialisasi Bahaya Phishing dan Tips Aman Menggunakan Internet bagi Mahasiswa Ilmu Komputer Institut Bisnis dan Komputer Indonesia” telah dilaksanakan dengan lancar pada hari Sabtu, 15 April 2025, bertempat di ruang pertemuan Gedung 1 Lantai 2 Kampus Institut Bisnis dan Komputer Indonesia. Peserta kegiatan ini berjumlah 30 mahasiswa dari Program Studi Ilmu Komputer semester 4, yang merupakan target utama kegiatan berdasarkan tingkat kebutuhan akan literasi keamanan digital mereka.

Kegiatan dimulai pada pukul 09.00 WIB dengan sesi pembukaan yang dilanjutkan sambutan dari dosen pembimbing pengabdian masyarakat. Selanjutnya, kegiatan inti dilaksanakan dalam bentuk sosialisasi interaktif yang dipandu oleh tim pelaksana dan narasumber. Materi yang disampaikan mencakup pemahaman mengenai phishing, jenis-jenis serangan phishing, contoh kasus nyata, serta tips pencegahan. Penyampaian dilakukan menggunakan media visual berupa slide PowerPoint, video pendek edukatif, dan simulasi email phishing. Metode ini dipilih untuk memberikan pemahaman secara teoritis sekaligus praktik langsung kepada peserta.

Gambar 1. Dokumentasi Narasumber Dengan Peserta Kegiatan

a. Hasil Pre-test

Sebelum sosialisasi dimulai, seluruh peserta diminta untuk mengisi lembar pre-test yang terdiri dari 10 soal pilihan ganda. Tujuan dari pre-test ini adalah untuk mengukur tingkat pemahaman awal peserta mengenai topik phishing dan keamanan digital. Hasil yang diperoleh menunjukkan bahwa sebagian besar peserta belum memiliki pengetahuan yang cukup mengenai topik ini. Dari total 30 peserta 21 orang (70%) menjawab kurang dari 6 soal dengan benar. Ini menunjukkan bahwa mayoritas peserta belum memahami bentuk-bentuk serangan phishing yang umum, seperti email palsu, tautan berbahaya, atau situs tiruan. 9 orang (30%) mampu menjawab 6 hingga 8 soal dengan benar, namun sebagian besar hanya mengandalkan intuisi, bukan pemahaman yang sistematis. Beberapa peserta mengira bahwa semua situs dengan logo resmi pasti aman, dan tidak mengetahui bahwa domain palsu bisa menyerupai situs asli (contoh: go0gle.com vs google.com). Temuan ini menegaskan bahwa dibutuhkan edukasi yang lebih mendalam agar peserta tidak menjadi korban kejahatan siber karena kurangnya literasi keamanan digital.



Gambar 2. Grafik Hasil Pre-test Pemahaman Phising Peserta

b. Hasil Pelaksanaan Sosialisasi

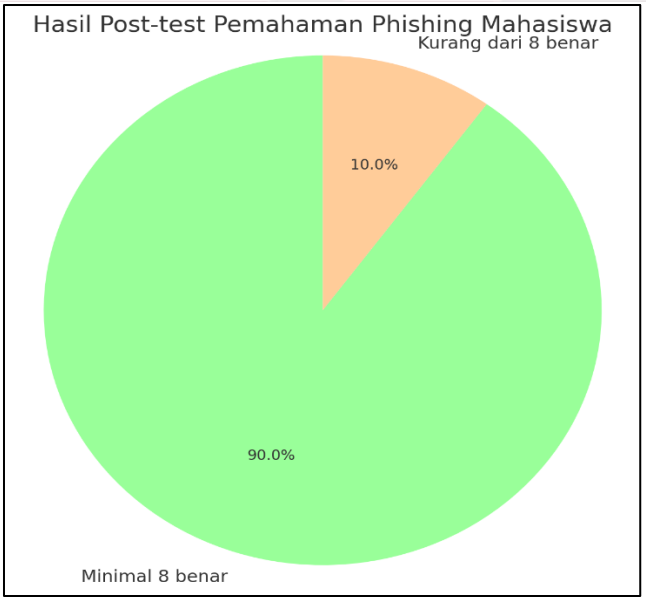
Sesi sosialisasi berjalan dengan sangat interaktif dan dinamis. Narasumber menyampaikan materi menggunakan pendekatan yang komunikatif, disertai ilustrasi visual, infografis, dan studi kasus nyata yang pernah terjadi di Indonesia. Materi disampaikan dalam tiga bagian utama: Pemahaman dasar tentang phishing: definisi, sejarah, dan mengapa metode ini sangat efektif digunakan oleh penjahat siber. Jenis-jenis phishing: seperti email phishing, spear phishing, vishing (voice phishing), dan smishing (SMS phishing). Tips aman menggunakan internet: seperti verifikasi tautan, tidak membagikan data pribadi sembarangan, mengenali email mencurigakan, serta pentingnya autentikasi dua faktor (2FA). Peserta juga diajak untuk mengikuti simulasi interaktif. Dalam sesi ini, ditampilkan dua contoh email satu asli dan satu palsu untuk dianalisis bersama. Peserta diminta menyebutkan ciri-ciri mencurigakan, seperti penggunaan alamat email yang tidak umum, adanya permintaan data pribadi, serta tautan yang tidak mengarah ke domain resmi. Respon peserta sangat positif. Banyak dari mereka menyadari bahwa selama ini mereka pernah menerima email serupa namun tidak tahu bahwa itu termasuk phishing. Kegiatan ini juga membangun kesadaran peserta agar lebih berhati-hati dan waspada dalam aktivitas digital sehari-hari.

c. Hasil Post-test

Setelah kegiatan sosialisasi dan simulasi selesai, peserta kembali diminta mengisi lembar post-test yang berisi 10 soal yang sama seperti pre-test, untuk mengevaluasi peningkatan pemahaman mereka. Hasil post-test menunjukkan peningkatan signifikan: 27 peserta (90%) mampu menjawab minimal 8 dari 10 soal dengan benar. Sebagian besar peserta kini mampu membedakan email phishing dan email resmi hanya dengan melihat struktur bahasa, domain pengirim, serta permintaan dalam isi pesan. Peningkatan nilai rata-rata peserta mencapai 40% lebih tinggi dibanding pre-test. Peserta juga memberikan testimoni singkat bahwa mereka merasa lebih percaya diri dan berhati-hati dalam menggunakan internet setelah mengikuti kegiatan ini.

Peningkatan hasil post-test menunjukkan bahwa metode penyampaian yang digunakan kombinasi antara teori, simulasi, dan diskusi terbukti efektif dalam meningkatkan literasi keamanan digital peserta. Hasil ini menjadi dasar bahwa kegiatan serupa perlu dilanjutkan secara rutin dengan cakupan audiens yang lebih luas.

Jurnal Pengabdian Kepada Masyarakat
Teknologi Informasi dan Komunikasi (PKM-TIK)
E-ISSN :3090-1588 (Online)



Gambar 3. Grafik Hasil Post-test Pemahaman Phising Peserta

5. KESIMPULAN

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi digital mahasiswa, khususnya dalam mengenali dan menghindari serangan phishing yang semakin marak terjadi di era digital saat ini. Berdasarkan hasil pre-test, mayoritas peserta masih memiliki pemahaman yang rendah terkait phishing, dengan 70% peserta menjawab kurang dari 6 soal dengan benar. Setelah dilakukan sosialisasi yang dikombinasikan dengan simulasi dan diskusi interaktif, terjadi peningkatan signifikan pada hasil post-test. Sebanyak 90% peserta mampu menjawab minimal 8 soal dengan benar, menunjukkan bahwa metode pembelajaran yang diterapkan efektif dalam menumbuhkan pemahaman serta kewaspadaan terhadap bahaya phishing. Selain peningkatan skor, peserta juga menunjukkan perubahan sikap, seperti lebih teliti dalam mengevaluasi email dan situs web, serta lebih berhati-hati dalam membagikan informasi pribadi di internet. Testimoni peserta menguatkan bahwa kegiatan ini memberikan manfaat nyata dan meningkatkan rasa percaya diri dalam menjaga keamanan digital mereka. Berdasarkan hasil dan tanggapan yang diperoleh, kegiatan ini terbukti bermanfaat dan layak untuk dilanjutkan secara rutin. Diharapkan kegiatan serupa dapat dilaksanakan dengan cakupan yang lebih luas, tidak hanya untuk mahasiswa tetapi juga untuk masyarakat umum guna membentuk ekosistem digital yang aman dan sadar akan ancaman siber.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada seluruh pihak yang telah mendukung pelaksanaan kegiatan pengabdian kepada masyarakat ini. Terutama kepada Institut Bisnis dan Komputer Indonesia, yang telah memberikan fasilitas dan izin pelaksanaan kegiatan, serta kepada mahasiswa Program Studi Ilmu Komputer Semester 4 yang telah berpartisipasi aktif dalam setiap sesi sosialisasi dan simulasi.

DAFTAR PUSTAKA

Aska, M. F., D. P. Putra, dan C. J. M. Sinambela. 2024. Strategi efektif untuk implementasi keamanan siber di era digital. *Journal of Informatic and Information Security*. 5(2):187–200.

Budiono, B., F. R. Fadillah, dan N. Arinudin. 2025. The dangers of phishing to personal data security. *Formosa Journal of Applied Sciences*. 4(3):831–844.

Dharani, L. I. C., S. Idayanti, dan K. Rahayu. 2024. *Perlindungan Hukum Terhadap Tindakan Phishing Di Media Sosial*. Penerbit NEM.

Huraerah, A. J. A., A. W. Abdullah, dan A. Rivai. 2024. Pengaruh teknologi informasi dan komunikasi terhadap pendidikan indonesia. *Journal of Islamic Education Policy*. 8(2)

Kainde, Q. C., J. S. Tambanaung, V. T. Inkiriwang, dan A. A. P. Mile. 2024. FORENSIC analysis of phishing attacks: investigative approach. *Jurnal Teknik Informatika (Jutif)*. 5(4):631–640.

Purba, A. 2023. Implementasi hasil pembelajaran dan peranannya dalam interaksi generasi digital native di media sosial. *Jurnal Suluh Pendidikan*. 11(1):40–54.

Ratutara, A. N. dan Y. Yusuf. 2025. Pengaruh tagline â€ œgratis ongkirâ€ market place shopee terhadap minat beli gen z di kota tangerang

selatan. *Holistic Journal of Management Research*. 10(1):1–9.

Samsumar, L. D., S. Nasiroh, S. Farizy, C. Anwar, I. H. Mursyidin, R. Rosdiyanto, W. W. Widiyanto, R. A. Mutiarawan, R. Mukin, dan T. Yusnanto. 2025. Keamanan Sistem Informasi: Perlindungan Data Dan Privasi Di Era Digital. 2025.

Situmorang, D. Y. 2023. Penggunaan media sosial sebagai alat bantu pembelajaran dan pengaruhnya terhadap interaksi siswa. *Jurnal Teknologi Pendidikan*. 2(2):110–119.

Surya, I. A. M. dan N. L. A. Moramowati. 2023. Efektivitas penggunaan teknologi dalam pendidikan terhadap kinerja akademik. *Metta: Jurnal Ilmu Multidisiplin*. 3(4):531–545.