Jurnal Pengabdian Masyarakat Ilmu Komputer
Volume 3, No 1 – Januari 2026
e-ISSN : 3046-8493

SOSIALISASI KEAMANAN DIGITAL DALAM UPAYA MENCEGAH PENIPUAN DARING DI KALANGAN MAHASISWA ASRAMA MAHASISWA NUSANTARA

Alif Raehan Maulana Muchtar*[1], Rafael Christian Marbun[2], Mochammad Arif Taufiqurrahman[3], Kristian Yosua Saputra[4], Muhammad Faruq Ramizi[5], Arulintang Divangga[6]
[123456]Telkom University Surabaya, Indonesia
alifraehan@student.telkomuniversity.ac.id[1], email@email.com[2]

Received: 20-12- 2025	Revised: 10-01-2026	Approved: 20-01-2026

ABSTRAK

Pesatnya perkembangan teknologi digital meningkatkan risiko penipuan daring, terutama di kalangan mahasiswa yang aktif menggunakan internet untuk keperluan akademik dan sosial. Mahasiswa yang tinggal pada Asrama Mahasiswa Nusantara menjadi salah satu kelompok rentan akibat kurangnya pemahaman tentang keamanan digital. Oleh karena itu, program sosialisasi ini bertujuan meningkatkan kesadaran mahasiswa mengenai ancaman penipuan daring serta memberikan strategi perlindungan yang efektif. Sosialisasi dilakukan melalui materi interaktif yang membahas jenis-jenis penipuan daring seperti phishing, memanipulasi, dan pencurian identitas. Mahasiswa diajarkan langkah-langkah pencegahan seperti penggunaan verifikasi dua langkah, pembuatan kata sandi kuat, serta kewaspadaan terhadap tautan mencurigakan. Selain itu, sesi simulasi kasus nyata dan diskusi kelompok diterapkan untuk memperkuat pemahaman praktis mahasiswa terhadap ancaman digital. Hasil yang diharapkan adalah peningkatan signifikan dalam pemahaman dan kewaspadaan mahasiswa terhadap modus penipuan daring. Program ini juga diharapkan menjadi langkah awal dalam membangun budaya literasi digital yang kuat di Asrama Mahasiswa Nusantara, sehingga mahasiswa dapat beraktivitas di dunia digital dengan lebih aman dan bijak.

***Kata Kunci**: Keamanan Digital; Penipuan Daring*

PENDAHULUAN

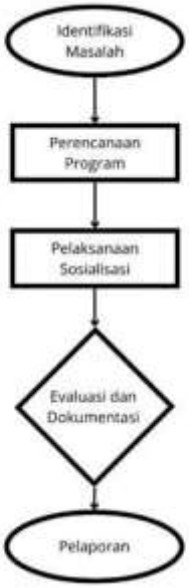
Perkembangan teknologi digital telah memberikan banyak manfaat dalam berbagai aspek kehidupan, termasuk di bidang akademik dan sosial. Mahasiswa sebagai generasi muda yang aktif dalam dunia digital memanfaatkan internet untuk mengakses informasi, berkomunikasi, serta melakukan transaksi secara daring. Namun, di balik kemudahan tersebut, terdapat risiko yang semakin meningkat, salah satunya adalah penipuan daring yang dapat merugikan secara finansial maupun privasi pengguna.

Mahasiswa Asrama Mahasiswa Nusantara, yang berasal dari berbagai daerah di Indonesia, sering kali kurang memiliki pemahaman yang memadai mengenai ancaman siber. Minimnya kesadaran akan pentingnya keamanan digital membuat mereka rentan menjadi target kejahatan siber, seperti phishing, social engineering, dan pencurian data pribadi. Berbagai modus penipuan daring terus berkembang dengan teknik yang semakin canggih, sehingga tanpa edukasi yang tepat, mahasiswa dapat dengan mudah terjebak dalam skema penipuan tersebut.

Oleh karena itu, diperlukan upaya pencegahan melalui sosialisasi keamanan digital guna meningkatkan pemahaman dan kewaspadaan mahasiswa terhadap potensi ancaman siber. Melalui program ini, mahasiswa akan diberikan edukasi mengenai berbagai jenis penipuan daring serta strategi perlindungan yang efektif. Diharapkan,

sosialisasi ini dapat membantu mahasiswa mengembangkan kebiasaan yang lebih aman dalam beraktivitas di dunia digital serta membangun budaya literasi digital yang lebih kuat di lingkungan Asrama Mahasiswa Nusantara.

METODE KEGIATAN



Metode yang digunakan dalam program pengabdian masyarakat ini dirancang secara komprehensif dan sistematis dengan mempertimbangkan karakteristik serta kebutuhan mahasiswa Asrama Mahasiswa Nusantara. Pendekatan yang diterapkan bersifat partisipatif dan interaktif, sehingga peserta tidak hanya menerima informasi, tetapi juga dapat memahami serta menerapkan konsep keamanan digital dalam kehidupan sehari-hari. Program ini dirancang agar memberikan dampak jangka panjang dalam meningkatkan literasi digital dan kewaspadaan terhadap ancaman penipuan daring.

Metode yang digunakan dalam sosialisasi ini mencakup beberapa tahap utama, yaitu:

1. Penyampaian Materi
   - Sesi presentasi interaktif mengenai berbagai modus penipuan daring seperti phishing, social engineering, dan pencurian identitas.
   - Pembahasan strategi perlindungan dengan menekankan penggunaan verifikasi dua langkah, pembuatan kata sandi yang kuat, serta cara mengenali tautan mencurigakan.
   - Penggunaan studi kasus nyata yang relevan dengan kehidupan mahasiswa untuk meningkatkan pemahaman terhadap ancaman digital.
2. Diskusi dan Tanya Jawab
   - Diskusi kelompok untuk mengidentifikasi risiko keamanan digital yang sering terjadi di lingkungan mahasiswa.
   - Sesi tanya jawab yang memungkinkan peserta menggali lebih dalam terkait pengalaman pribadi maupun permasalahan keamanan digital yang mereka hadapi.

3. Evaluasi Pemahaman
   - Pelaksanaan kuis interaktif menggunakan platform Google from untuk mengukur sejauh mana pemahaman peserta terhadap materi yang disampaikan.
   - Pemberian reward bagi peserta dengan nilai tertinggi untuk meningkatkan motivasi dan partisipasi dalam kegiatan.
4. Pengukuran Keberhasilan Program
   - Peningkatan pemahaman, dengan target minimal 75% peserta mencapai skor di atas 70 pada evaluasi kuis.

HASIL DAN PEMBAHASAN

Pelaksanaan program sosialisasi keamanan digital di Asrama Mahasiswa Nusantara menunjukkan hasil yang positif dan memberikan dampak nyata terhadap peningkatan literasi digital para peserta. Temuan ini sejalan dengan studi(Kaleli, 2024) yang menunjukkan bahwa mahasiswa perguruan tinggi memiliki tingkat kesadaran keamanan digital pada level menengah ke atas, terutama dalam hal praktik dasar seperti keamanan kata sandi dan penggunaan internet yang aman. Studi tersebut menekankan perlunya pendekatan edukatif berbasis kebutuhan nyata mahasiswa untuk memperkuat perlindungan data digital mereka Kegiatan ini dirancang untuk tidak hanya menyampaikan informasi, tetapi juga membentuk pemahaman praktis melalui partisipasi aktif mahasiswa dalam diskusi, studi kasus, dan evaluasi.

Program ini dilaksanakan secara tatap muka dalam suasana informal namun edukatif, yang mendorong interaksi dua arah antara fasilitator dan peserta. Peserta kegiatan terdiri dari 45 mahasiswa dengan latar belakang daerah dan jurusan yang beragam, mencerminkan heterogenitas karakteristik penghuni asrama.

Gambar 1. Penyampaian Materi

Sesi pertama kegiatan berupa penyampaian materi mengenai bentuk-bentuk penipuan daring yang umum terjadi di kalangan mahasiswa, seperti *phishing*, manipulasi sosial (*social engineering*), serta pencurian identitas digital. Materi ini disampaikan secara interaktif menggunakan media presentasi visual, video pendek, dan infografik. Mahasiswa diajak untuk mengidentifikasi modus-modus penipuan yang mungkin mereka temui dalam keseharian, seperti email palsu yang mengatasnamakan

institusi resmi, pesan singkat dari akun media sosial yang berpura-pura sebagai teman, hingga undangan rapat atau beasiswa fiktif yang mencurigakan. Pemaparan materi juga dilengkapi dengan strategi pencegahan, seperti pentingnya penggunaan kata sandi yang kompleks dan unik, penerapan verifikasi dua langkah pada akun digital, serta cara memeriksa keaslian tautan dan alamat situs web.

Menariknya, ketika disampaikan contoh kasus penipuan yang pernah terjadi di kalangan mahasiswa, sebagian peserta mengakui bahwa mereka pernah hampir menjadi korban, dan bahkan ada yang sempat mengalami kerugian finansial dalam jumlah kecil. Hal ini sejalan dengan temuan (Bottyán, 2024), yang menunjukkan bahwa meskipun sebagian besar mahasiswa merasa aman saat beraktivitas di dunia digital, banyak di antaranya telah mengalami insiden keamanan siber seperti percobaan penipuan atau pelanggaran akun Hal ini menunjukkan bahwa fenomena penipuan daring bukanlah sesuatu yang asing atau jauh dari realita mereka. Dalam diskusi kelompok yang difasilitasi oleh panitia, para peserta menceritakan pengalaman pribadi dan saling bertukar informasi mengenai upaya mereka dalam melindungi data pribadi. Banyak peserta menyadari bahwa mereka masih menggunakan kata sandi yang sama untuk berbagai akun, atau belum mengaktifkan fitur keamanan tambahan seperti *two-factor authentication* (2FA), yang padahal dapat sangat membantu dalam mengamankan akun. Evaluasi melalui kuis juga mencerminkan pendekatan yang sejalan dengan penelitian(Bognár & Bottyán, 2024), yang mengembangkan skala validasi untuk mengukur perilaku keamanan digital mahasiswa, serta menekankan pentingnya memahami dimensi perilaku nyata seperti penggunaan kata sandi dan aktivasi autentikasi ganda sebagai bagian dari peningkatan kesadaran siber yang efektif

Gambar 2. Sesi Kuis

Setelah sesi penyampaian materi dan diskusi, dilakukan evaluasi pemahaman menggunakan kuis daring yang terdiri dari 15 pertanyaan seputar konten yang telah dipelajari. Kuis ini tidak hanya berfungsi sebagai alat ukur pemahaman, tetapi juga sebagai refleksi langsung bagi peserta terhadap apa yang mereka serap selama kegiatan berlangsung. Berdasarkan data dari hasil kuis, sebanyak 82% peserta berhasil memperoleh skor di atas 70, yang menjadi indikator utama keberhasilan program. Rata-rata nilai keseluruhan peserta adalah 78,6, yang mencerminkan bahwa mayoritas peserta telah memahami konsep dasar penipuan daring dan strategi perlindungan yang dibahas. Topik yang paling banyak dijawab dengan benar adalah tentang ciri-ciri email phishing dan praktik kata sandi yang aman. Sebaliknya, beberapa peserta tampak masih

kesulitan memahami pentingnya penggunaan *password manager* serta cara teknis memverifikasi keaslian URL.

Selain itu, untuk meningkatkan semangat dan partisipasi, panitia menyediakan apresiasi bagi peserta dengan skor tertinggi berupa sertifikat dan hadiah simbolis. Hal ini terbukti efektif dalam meningkatkan antusiasme peserta, sebagaimana tercermin dari feedback yang diberikan. Dalam survei singkat yang dibagikan setelah kegiatan, mayoritas peserta menyatakan bahwa kegiatan ini sangat bermanfaat dan membuka wawasan baru bagi mereka. Temuan ini diperkuat oleh penelitian (Latorre-Medina & Tnibar-Harrus, 2023), yang menemukan bahwa meskipun peserta pelatihan pendidikan merasa cukup kompeten secara teknologis, mereka mengakui masih membutuhkan pelatihan lebih mendalam mengenai keamanan digital, terutama dalam hal penerapan praktis. Banyak yang berharap agar kegiatan serupa dilakukan secara berkala dan diperluas ke topik-topik lain seperti perlindungan data di media sosial, keamanan transaksi digital, dan cara mendeteksi hoaks. Harapan peserta agar kegiatan ini dilakukan secara berkala sejalan dengan pendekatan yang diusulkan oleh Siahaan & Tampubolon (2024), yang menekankan pentingnya kolaborasi antarelemen kampus dan integrasi literasi digital ke dalam kebijakan dan kurikulum sebagai upaya jangka panjang untuk membangun lingkungan pendidikan yang aman dan responsif secara digita(Siahaan & Tampubolon, 2024).

Secara keseluruhan, keberhasilan program ini tidak hanya tercermin dari skor evaluasi, tetapi juga dari perubahan sikap dan peningkatan kesadaran peserta terhadap pentingnya menjaga keamanan identitas digital. Interaksi aktif dalam diskusi, pengakuan pengalaman pribadi peserta, serta keterbukaan terhadap perubahan perilaku digital menunjukkan bahwa pendekatan sosialisasi yang digunakan telah tepat sasaran. Program ini memberikan bukti bahwa dengan metode yang partisipatif dan relevan secara kontekstual, pemahaman mahasiswa terhadap isu keamanan digital dapat ditingkatkan secara signifikan.

Gamabar 3. Sesi Foto Bersama

KESIMPULAN

Kegiatan sosialisasi keamanan digital yang dilaksanakan di Asrama Mahasiswa Nusantara memberikan dampak yang signifikan dalam meningkatkan pengetahuan dan

kesadaran mahasiswa terhadap ancaman penipuan daring. Dalam era digital saat ini, mahasiswa merupakan salah satu kelompok pengguna internet yang paling aktif, namun tidak selalu disertai dengan pengetahuan yang memadai mengenai risiko yang ada di dunia maya. Melalui program ini, peserta tidak hanya dikenalkan dengan berbagai modus penipuan digital seperti *phishing*, manipulasi sosial, dan pencurian identitas, tetapi juga diberikan pemahaman praktis tentang bagaimana melindungi diri dari ancaman tersebut.

Pendekatan yang digunakan dalam kegiatan ini terbukti efektif. Penyampaian materi dilakukan secara interaktif dan kontekstual, disesuaikan dengan pengalaman serta kebutuhan sehari-hari mahasiswa. Hal ini mendorong keterlibatan aktif peserta, baik dalam sesi tanya jawab, diskusi kelompok, maupun dalam pengisian evaluasi. Melalui studi kasus nyata, peserta mampu melihat relevansi antara materi yang disampaikan dengan situasi yang mereka hadapi dalam kehidupan digital sehari-hari, sehingga pemahaman yang dibentuk menjadi lebih bermakna dan aplikatif.

Hasil kuis evaluasi menunjukkan bahwa mayoritas peserta telah mencapai tingkat pemahaman yang baik, dengan 82% dari mereka memperoleh skor di atas ambang batas yang ditetapkan. Capaian ini mencerminkan bahwa materi telah berhasil disampaikan dengan baik dan diterima dengan cukup baik pula oleh peserta. Selain hasil kuantitatif, indikator keberhasilan juga tercermin dari tanggapan peserta yang antusias dan refleksi mereka terhadap pengalaman pribadi terkait keamanan digital. Banyak peserta menyatakan kesadaran barunya untuk mulai mengubah kebiasaan digital yang sebelumnya kurang aman, seperti mengganti kata sandi yang lemah, mengaktifkan fitur verifikasi dua langkah, serta lebih waspada terhadap tautan atau pesan mencurigakan.

Dari pelaksanaan kegiatan ini dapat disimpulkan bahwa literasi digital, khususnya dalam aspek keamanan dan perlindungan data pribadi, masih menjadi kebutuhan penting di kalangan mahasiswa. Kegiatan sosialisasi seperti ini sangat relevan dan perlu dilakukan secara berkelanjutan untuk memperkuat kesadaran kolektif mengenai pentingnya menjaga identitas digital dan mencegah kerugian akibat kejahatan siber. Diharapkan, kegiatan ini dapat menjadi pijakan awal bagi terbentuknya budaya digital yang aman, bijak, dan bertanggung jawab di lingkungan Asrama Mahasiswa Nusantara, serta menjadi model bagi pelaksanaan kegiatan serupa di lingkungan pendidikan lainnya.

DAFTAR PUSTAKA

Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*, *14*(6). https://doi.org/10.3390/educsci14060588

Bottyán, L. (2024). Feeling safe online and experience with cyber incidents among university students. *Gradus*, *11*(1). https://doi.org/10.47833/2024.1.csc.001

Kaleli, S. S. (2024). Measuring Digital Data Security Awareness: The Case of Higher Education Institution. *Journal of Studies in Advanced Technologies*, *2*(2), 108–119. https://doi.org/10.63063/jsat.1591281

Latorre-Medina, M. J., & Tnibar-Harrus, C. (2023). DIGITAL SECURITY IN EDUCATIONAL TRAINING PROGRAMS: A STUDY BASED ON FUTURE TEACHERS' PERCEPTIONS.

Information Technologies and Learning Tools, *95*(3), 102–111. https://doi.org/10.33407/itlt.v95i3.5204

Siahaan, R., & Tampubolon, R. C. (2024). Strengthening Digital Literacy and Internet Security Awareness for Sisingamngaraja XII Tapanuli University Students: Building Sustainable Policies and Practices in Higher Education Environments. *International Journal of Community Engagement and Development*, *2*(2), 9–14. https://doi.org/10.55606/ijced.widyakarya.v2i2.23