Jurnal Komputer Multidisipliner

Vol.8 No.4, April 2025
ISSN: 24559633

LITERASI DIGITAL DAN KEAMANAN SIBER DALAM DUNIA PENDIDIKAN: ANALISIS KESADARAN DAN PRAKTIK DI KALANGAN MAHASISWA

Uka Riski[1], Salman Al Farisi[2], Rafiq Fauzan[3], Eva Iryani[4], Helty[5]
Universitas Jambi
E-mail: ukareski61@gmail.com[1], salmanaris2006@gmail.com[2], rafiqfauzan903@gmail.com[3], evairyani@unja.ac.id[4], heltyasafri@unja.ac.id[5]

Abstrak

Perkembangan teknologi digital telah membawa perubahan signifikan dalam dunia pendidikan, meningkatkan aksesibilitas dan efisiensi pembelajaran. Namun, hal ini juga menimbulkan tantangan baru terkait keamanan siber, terutama bagi mahasiswa yang aktif menggunakan teknologi digital dalam aktivitas akademik mereka. Artikel ini bertujuan untuk menganalisis tingkat kesadaran dan praktik keamanan siber di kalangan mahasiswa dalam konteks literasi digital. Melalui kajian pustaka, ditemukan bahwa meskipun mahasiswa memiliki akses luas terhadap teknologi digital, masih terdapat celah dalam pemahaman dan implementasi praktik keamanan siber. Oleh karena itu, diperlukan upaya peningkatan kesadaran dan implementasi strategi keamanan digital yang lebih baik di lingkungan akademik.

Kata Kunci — Literasi Digital, Keamanan Siber, Pendidikan, Mahasiswa, Kesadaran Siber.

1. PENDAHULUAN

Teknologi digital telah menjadi bagian integral dalam dunia pendidikan modern, memungkinkan mahasiswa untuk mengakses informasi, berkomunikasi, dan menyelesaikan tugas akademik secara lebih efisien. Platform pembelajaran daring, sistem manajemen pembelajaran (Learning Management Systems/LMS), media sosial, serta berbagai aplikasi berbasis cloud telah mengubah cara mahasiswa belajar dan berinteraksi. Transformasi digital ini juga dipercepat oleh situasi global seperti pandemi COVID-19, yang mendorong adopsi teknologi secara masif dalam proses pembelajaran (Zalat, Hamed, and Bolbol 2021).

Namun, ketergantungan pada teknologi ini juga meningkatkan risiko terhadap ancaman siber seperti pencurian data, peretasan akun, serangan phishing, dan penyebaran malware. Mahasiswa, sebagai pengguna aktif teknologi, menjadi kelompok yang rentan apabila tidak memiliki pemahaman dan kewaspadaan yang cukup terhadap ancaman tersebut. Literasi digital tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga pemahaman tentang bagaimana melindungi informasi pribadi dan akademik di dunia maya (McGuinness and Fulton 2019).

Penelitian menunjukkan bahwa meskipun mahasiswa memiliki akses ke teknologi digital, mereka sering kali mengabaikan aspek keamanan dalam penggunaannya. Contohnya, banyak mahasiswa menggunakan kata sandi yang lemah atau berbagi informasi pribadi tanpa mempertimbangkan konsekuensinya (Alharbi and Tassaddiq 2021). Perilaku semacam ini menunjukkan rendahnya kesadaran terhadap pentingnya perlindungan data dan privasi di lingkungan digital, yang pada akhirnya meningkatkan kerentanan terhadap berbagai serangan siber.

Oleh karena itu, diperlukan kajian konseptual yang tidak hanya menjelaskan pentingnya literasi digital dan keamanan siber, tetapi juga menganalisis kesadaran dan

praktik mahasiswa dalam menghadapi tantangan digital. Artikel ini bertujuan untuk mengkaji konsep literasi digital dan keamanan siber dalam konteks pendidikan tinggi, dengan fokus pada sejauh mana mahasiswa memahami dan menerapkan prinsip-prinsip keamanan digital dalam kehidupan akademik mereka. Melalui pendekatan analisis literatur, tulisan ini diharapkan dapat memberikan kontribusi terhadap pengembangan strategi literasi digital yang lebih menyeluruh dan berkelanjutan di lingkungan pendidikan tinggi.

2. HASIL DAN PEMBAHASAN

Beberapa studi telah meneliti tingkat kesadaran keamanan siber di kalangan mahasiswa. Misalnya, penelitian oleh (Schoenmakers et al. 2023) menemukan bahwa banyak mahasiswa tidak menyadari pentingnya menggunakan kata sandi yang kuat dan unik untuk setiap akun mereka. Selain itu, penelitian oleh (Alharbi and Tassaddiq 2021) mengungkapkan bahwa sebagian besar mahasiswa tidak memahami risiko yang terkait dengan penggunaan jaringan Wi-Fi publik tanpa perlindungan yang memadai.

Dalam konteks kehidupan akademik, praktik keamanan siber yang baik sangat penting untuk melindungi data pribadi dan akademik. Namun, penelitian menunjukkan bahwa banyak mahasiswa tidak menerapkan langkah-langkah keamanan dasar (Bognár and Bottyán 2024). Sebagai contoh, studi oleh (Alharbi and Tassaddiq 2021) menemukan bahwa sebagian besar mahasiswa tidak secara rutin memperbarui perangkat lunak mereka, yang dapat meninggalkan celah keamanan.

Lebih jauh lagi, gaya hidup digital mahasiswa juga berdampak terhadap risiko keamanan. Menurut studi oleh (O'Day and Heimberg 2021) mahasiswa yang memiliki tingkat ketergantungan tinggi terhadap media sosial menunjukkan perilaku yang kurang berhati-hati, seperti berbagi informasi lokasi dan data pribadi secara publik. Hal ini memperbesar potensi eksploitasi data oleh pihak tidak bertanggung jawab. Oleh karena itu, pembinaan literasi digital seharusnya tidak hanya berfokus pada keterampilan teknis, tetapi juga pada pembangunan kesadaran kritis terhadap jejak digital.

Terakhir, terdapat kebutuhan untuk membangun budaya sadar keamanan digital di kalangan sivitas akademika. Seperti dijelaskan oleh (Mujiono 2024), kesadaran keamanan tidak bisa dibangun dalam waktu singkat, melainkan memerlukan proses pembiasaan yang terus-menerus melalui sosialisasi, simulasi kasus, dan penyusunan panduan penggunaan teknologi yang aman. Pendidikan literasi digital yang berorientasi pada keamanan tidak hanya meningkatkan kapasitas mahasiswa secara individu, tetapi juga memperkuat ketahanan siber institusi secara keseluruhan.

Selain pendekatan individual, penting pula untuk mempertimbangkan pendekatan sistemik dalam meningkatkan literasi digital dan keamanan siber di kalangan mahasiswa. Institusi pendidikan tidak hanya bertanggung jawab menyediakan infrastruktur digital yang aman, tetapi juga perlu mengintegrasikan edukasi keamanan siber ke dalam berbagai aspek kegiatan akademik. Pelatihan, seminar, dan simulasi kasus nyata dapat menjadi sarana efektif untuk membangun kesadaran kolektif serta memperkuat kemampuan mahasiswa dalam menghadapi berbagai ancaman siber. Dengan langkah-langkah tersebut, diharapkan terbentuk budaya digital yang tidak hanya cakap dalam penggunaan teknologi, tetapi juga waspada dan bertanggung jawab dalam menjaga keamanan data dan privasi.

Strategi Peningkatan Kesadaran dan Keamanan Siber bagi Mahasiswa

Untuk meningkatkan kesadaran dan praktik keamanan siber di kalangan mahasiswa, beberapa strategi dapat diterapkan:

1. Edukasi dan Pelatihan: Institusi pendidikan tinggi harus menyediakan program pelatihan yang berfokus pada keamanan siber, termasuk cara mengenali dan

menghindari ancaman siber (Kennison and Eric Chan-Tin 2023).

2. Kampanye Kesadaran: Mengadakan kampanye kesadaran secara rutin untuk mengingatkan mahasiswa tentang pentingnya keamanan siber (Alharbi and Tassaddiq 2021).
3. Integrasi Keamanan Siber dalam Kurikulum: Mengintegrasikan topik keamanan siber dalam mata kuliah yang relevan untuk memastikan bahwa mahasiswa mendapatkan pengetahuan yang diperlukan selama studi mereka (McGuinness & Fulton, 2019).
4. Penyediaan Sumber Daya dan Dukungan: Institusi harus menyediakan sumber daya seperti perangkat lunak keamanan gratis atau berlisensi, serta layanan dukungan teknis untuk membantu mahasiswa dalam mengatasi masalah keamanan siber(Bognár and Bottyán 2024).
5. Simulasi dan Studi Kasus: Melakukan simulasi insiden keamanan siber atau studi kasus nyata dapat membantu mahasiswa memahami dampak langsung dari kelalaian dalam menjaga keamanan digital. Pendekatan ini memungkinkan mereka belajar dari skenario yang realistis dan meningkatkan kesiapsiagaan dalam menghadapi situasi serupa.
6. Penerapan Kebijakan Keamanan Internal: Institusi dapat menetapkan kebijakan keamanan digital yang wajib dipatuhi oleh seluruh sivitas akademika, termasuk aturan penggunaan perangkat, akses jaringan, dan kebijakan kata sandi. Kebijakan ini juga perlu disosialisasikan secara aktif agar dipahami dan diterapkan dengan konsisten.
7. Penguatan Peran Organisasi Mahasiswa: Organisasi kemahasiswaan dapat dilibatkan sebagai agen perubahan dalam menyebarluaskan literasi keamanan siber. Melalui kegiatan, pelatihan, atau media sosial, mereka bisa membantu menjangkau lebih banyak mahasiswa secara informal namun berdampak.
8. Monitoring dan Evaluasi Berkala: Strategi yang diterapkan perlu dievaluasi secara berkala untuk mengetahui efektivitasnya. Survei, wawancara, atau pengamatan langsung dapat digunakan untuk mengukur sejauh mana mahasiswa mengalami peningkatan kesadaran dan praktik keamanan.

3. KESIMPULAN

Literasi digital dan keamanan siber merupakan aspek krusial dalam dunia pendidikan tinggi yang semakin bergantung pada teknologi digital. Meskipun mahasiswa memiliki akses luas terhadap perangkat dan platform digital, masih terdapat kesenjangan dalam pemahaman dan penerapan praktik keamanan siber yang baik. Kajian dalam artikel ini menunjukkan bahwa banyak mahasiswa kurang menyadari ancaman seperti phishing, pencurian data, dan serangan malware, serta tidak menerapkan langkah-langkah perlindungan yang memadai, seperti penggunaan kata sandi yang kuat atau pencadangan data secara berkala.

Untuk mengatasi tantangan ini, institusi pendidikan perlu mengambil langkah proaktif dalam meningkatkan kesadaran dan keterampilan keamanan siber di kalangan mahasiswa. Dengan adanya peningkatan kesadaran dan penerapan strategi keamanan yang lebih baik, mahasiswa dapat lebih terlindungi dari risiko siber dan dapat memanfaatkan teknologi digital secara aman dan efektif dalam lingkungan akademik.

DAFTAR PUSTAKA

Alharbi, Talal, and Asifa Tassaddiq. 2021. “Assessment of Cybersecurity Awareness among Students of Majmaah.”

Bognár, László, and László Bottyán. 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.

Bottyan, Laszlo. 2023. “Cybersecurity Awareness among University Students.” Journal of Applied

Technical and Educational Sciences JATES 13 (3): 1–11. https://doi.org/10.24368/jates363.
Kennison, Shelia M., and D. Eric Chan-Tin. 2023. “Personality and Cognitive Factors in Password Security Behaviors.” North American Journal of Psychology 25 (3): 599–618.
McGuinness, Claire, and Crystal Fulton. 2019. “Digital Literacy in Higher Education: A Case Study of Student Engagement with e-Tutorials Using Blended Learning.” Journal of Information Technology Education: Innovations in Practice 18: 1–28. https://doi.org/10.28945/4190.
Mujiono, Mujiono. 2024. “Digital Literacy: Fundamental Competence for Modern Society.” DIDAKTIKA: Jurnal Pemikiran Pendidikan 30 (1): 15. https://doi.org/10.30587/didaktika.v30i1.6906.
Musiin, Dan Indrajit, R.E. 2020. “Literasi Digital Nusantara-Meningkatkan Daya Saing Generasi Muda.” Literasi Digital Nusantara-Meningkatkan Daya Saing Generasi Muda 14 (1): 54–65.
O’Day, Emily B., and Richard G. Heimberg. 2021. “Social Media Use, Social Anxiety, and Loneliness: A Systematic Review.” Computers in Human Behavior Reports 3 (October 2020): 100070. https://doi.org/10.1016/j.chbr.2021.100070.
Schoenmakers, Koen, Daniel Greene, Sarah Stutterheim, Herbert Lin, and Megan J. Palmer. 2023. “The Security Mindset: Characteristics, Development, and Consequences.” Journal of Cybersecurity 9 (1): 1–15. https://doi.org/10.1093/cybsec/tyad010.
Zalat, Marwa Mohamed, Mona Sami Hamed, and Sarah Abdelhalim Bolbol. 2021. “The Experiences, Challenges, and Acceptance of e-Learning as a Tool for Teaching during the COVID-19 Pandemic among University Medical Staff.” PLoS ONE 16 (3 March): 1–12. https://doi.org/10.1371/journal.pone.0248758.