Pengetahuan Mahasiswa Mengenai Isu Keamanan Sekuriti pada Pusat Data Nasional : Ransomware

Latifah Iriani[1], Rakhmat Prasetyo Agung[2], Joko Supriyanto[3], Andi Sugandi[4], Muhammad Immawan Aulia[5]
[1, 2, 3, 4] Informatika, Universitas Siber Muhammadiyah, Yogyakarta, Indonesia
[5] Informatika, Universitas Islam Mulia Yogyakarta, Yogyakarta, Indonesia
Email: [1]latifahiriani@sibermu.ac.id, [2] agungprasetyo@sibermu.ac.id, [3]joko@sibermu.ac.id, [4]andi@sibermu.ac.id, [5]muhimmawanaulia16@uimyogya.ac.id

***Abstract*—Pusat Data Nasional (PDN) memiliki peran penting dalam penyimpanan dan pengelolaan data pemerintah maupun publik, menjadikannya target strategis bagi ancaman keamanan siber seperti ransomware. Penelitian ini bertujuan untuk mengukur tingkat pengetahuan mahasiswa terkait isu keamanan PDN, khususnya ancaman ransomware, sebelum dan sesudah mengikuti rangkaian webinar. Metode yang digunakan adalah pre-test dan post-test dengan sampel mahasiswa dari Universitas Siber Muhammadiyah dan Universitas Islam Mulia Yogyakarta. Hasil penelitian menunjukkan adanya peningkatan signifikan dalam pengetahuan mahasiswa setelah mengikuti webinar, yang dipengaruhi oleh latar belakang pendidikan, frekuensi penggunaan teknologi, dan partisipasi aktif dalam diskusi. Kesimpulannya, webinar series terbukti efektif dalam meningkatkan literasi keamanan siber mahasiswa. Penelitian ini merekomendasikan integrasi pendidikan keamanan siber ke dalam kurikulum, serta penyelenggaraan lebih banyak webinar untuk meningkatkan kesadaran mahasiswa terhadap isu keamanan digital yang semakin kompleks.**

Keywords—National Data Center (PDN); Ransomware; Cybersecurity Awareness

I. PENDAHULUAN

Perkembangan teknologi digital yang pesat telah membawa transformasi besar dalam berbagai sektor, termasuk dalam aspek pertahanan dan keamanan nasional. Ancaman siber yang semakin kompleks dan terorganisir menjadi tantangan serius bagi kedaulatan negara, infrastruktur kritis, serta perlindungan data publik dan pemerintahan [1]. Menurut BSSN, pembangunan Pusat Data Nasional dirancang untuk mendukung industri nasional dan memperkuat ketahanan data pemerintah dengan standar keamanan yang berlapis [2] .

Dengan meningkatnya ketergantungan pada sistem digital, PDN menjadi salah satu target utama serangan siber, terutama serangan ransomware yang dapat mengunci akses terhadap data penting dan menuntut tebusan untuk pemulihannya [3] [4] . Menurut laporan IMF dan studi akademik dalam *Asian Journal of Economics, Business and Accounting*, serangan siber seperti ransomware dapat mengancam kedaulatan dan stabilitas nasional melalui kerugian finansial besar dan gangguan layanan infrastruktur kritis [3].

Meningkatkan kesadaran dan literasi keamanan siber, khususnya di kalangan mahasiswa, menjadi sangat penting mengingat mereka adalah generasi penerus tenaga kerja digital [5]. Mahasiswa perlu dibekali pengetahuan tentang ancaman siber dan strategi mitigasinya agar mampu berkontribusi dalam memperkuat ketahanan digital nasional [5].

Dalam upaya membangun ketahanan tersebut, pendekatan edukatif seperti penyelenggaraan webinar dinilai efektif untuk memberikan pemahaman praktis dan konseptual mengenai isu-isu keamanan informasi. Kementerian Komunikasi dan Informatika bahkan menekankan urgensi pembentukan angkatan siber yang profesional, termasuk melalui peningkatan kapasitas SDM di bidang keamanan digital dan pembentukan tim tanggap insiden siber nasional [6]. Penelitian menyebutkan bahwa pengembangan SDM siber nasional melalui BSSN memperhatikan berbagai faktor strategis dan melibatkan pelatihan teknis, sertifikasi profesi, serta tim Tanggap Insiden Siber sebagai pilar utama kesiapsiagaan nasional [7].

Penelitian ini dilakukan untuk mengeksplorasi sejauh mana pengetahuan mahasiswa mengenai isu keamanan sekuriti, khususnya pada Pusat Data Nasional, dengan fokus pada ancaman ransomware. Melalui rangkaian webinar series, mahasiswa dari Universitas Siber Muhammadiyah dan Universitas Islam Mulia Yogyakarta diikutsertakan untuk mendapatkan pemahaman yang lebih baik tentang praktik terbaik dalam keamanan siber. Hasil dari penelitian ini diharapkan dapat menjadi dasar pengembangan strategi edukasi keamanan digital yang lebih luas di lingkungan pendidikan tinggi.

II. LITERATUR REVIEW

Beberapa studi menyoroti tingginya ancaman ransomware terhadap infrastruktur penting. Misalnya, Puspita et al. (2025) menganalisis serangan Brain Cipher (LockBit 3.0) pada Pusat Data Nasional sementara, yang melumpuhkan layanan publik di 282 instansi [8].

Mereka menilai ancaman ini sebagai “kritis” karena lemahnya tata kelola, minimnya cadangan data, dan rendahnya kesadaran keamanan [8]. Penelitian tersebut menegaskan bahwa upaya mitigasi memerlukan peningkatan

manajemen risiko dan pelatihan keamanan siber nasional [8]. Dalam konteks lebih luas, temuan ini menggambarkan betapa ransomware merupakan ancaman serius pada pusat data dan infrastruktur digital, sekaligus menunjukkan perlunya literasi keamanan siber yang kuat.

A. Metode Edukatif untuk Meningkatkan Kesadaran

Berbagai riset menerapkan pelatihan interaktif untuk meningkatkan kesadaran mahasiswa tentang keamanan siber. Misalnya:

- Surdjono et al. (2025) mengembangkan program *mobile learning* khusus bagi mahasiswa akuntansi dan keuangan. Hasil evaluasi menunjukkan peningkatan signifikan dalam kesadaran siber dan praktik cyber hygiene setelah program tersebut diterapkan [9]. Program ini memanfaatkan konten interaktif (modul, simulasi, forum diskusi) yang dirancang sesuai kebutuhan mahasiswa.
- Sarungu et al. (2023) mengadakan seminar literasi keamanan di Universitas Slamet Riyadi. Dalam evaluasi dilakukan pre-test dan post-test wawancara, peneliti melaporkan bahwa setelah seminar "pengetahuan peserta […] meningkat drastis" dibandingkan sebelum materi disampaikan (misalnya pemahaman tentang ketiadaan UU Perlindungan Data Pribadi) [10] . Hasil ini menunjukkan bahwa workshop/seminar dapat memperkuat pemahaman mahasiswa tentang ancaman dan perlindungan data pribadi.
- Samonte et al. (2023) mengembangkan modul e-learning asisten untuk mahasiswa Filipina (dilengkapi teks-berbicara dan laboratorium virtual). Dengan membandingkan dua kelompok post-test, mereka menemukan mahasiswa yang menggunakan modul interaktif ini meraih skor lebih tinggi dibanding kelompok yang belajar konvensional [11]. Ini menegaskan efektivitas platform daring interaktif dalam meningkatkan pembelajaran keamanan siber.
- Mohuyula (2025) melaporkan pelatihan literasi digital (penggunaan komputer dan internet aman) di sebuah panti asuhan. Rata-rata skor pre-test sangat rendah (30%), tetapi meningkat menjadi 75% pada post-test setelah pelatihan [12]. Skor ini menggambarkan kenaikan pemahaman peserta secara signifikan berkat sesi pelatihan praktis.

Temuan-temuan di atas menekankan bahwa penggunaan metode edukatif (mobile learning, seminar, workshop, modul daring) terbukti meningkatkan literasi keamanan siber. Selain itu, survei oleh Humaira et al. (2024) di kampus menggarisbawahi pentingnya peran institusi (penyediaan informasi rutin dan pelatihan) sebagai agen perubahan dalam menaikkan kesadaran siber mahasiswa [13].

B. Pendekatan Pre-test/Post-test

Banyak studi mengukur efektivitas intervensi edukatif dengan desain *pre-test* dan *post-test*. Seperti :

- Surdjono et al. (2025) secara eksplisit menyatakan memberikan *pre-test* kepada mahasiswa sebelum program mobile learning dan *post-test* setelahnya untuk mengukur peningkatan pemahaman keamanan siber. Hasilnya, ada peningkatan signifikan skor dan praktek keamanan (cyber hygiene) setelah intervensi [9].
- Sarungu et al. (2023) menggunakan pertanyaan *pre-test* (wawancara singkat) lalu *post-test* setelah seminar. Mereka mencatat peningkatan drastis pemahaman mahasiswa tentang topik keamanan yang diajarkan [10].
- Mohuyula (2025) menunjukkan penggunaan kuis pre-test/post-test sederhana di akhir sesi literasi digital. Sebelum pelatihan, skor rata-rata hanya ~30%, kemudian naik menjadi 75% pada post-test, menandakan efektivitas materi [12].

Pendekatan ini umum karena mampu menilai secara kuantitatif dampak intervensi. Keberhasilan signifikan (misalnya lonjakan skor 30%→75%) memperkuat rekomendasi bahwa pelatihan berstruktur memberikan peningkatan literasi siber nyata bagi peserta.

C. Perbandingan dengan Literatur Sebelumnya (Novelty)

Studi-studi terdahulu sebagian besar fokus pada kesadaran umum keamanan siber dan efektivitas pelatihan, tetapi belum membahas khusus topik ransomware di konteks infrastruktur nasional. Misalnya, Tan dkk. (2024) hanya menilai kebiasaan keamanan dasar (password, data pribadi) mahasiswa di Batam [13]; Garba dkk. (2021) mengukur literasi siber mahasiswa Nigeria secara umum [14]; dan Humaira dkk. (2024) melaporkan tingkat pengetahuan mahasiswa dasar tentang keamanan siber [15]. Sementara itu, program-program intervensi (Surdjono 2025, Sarungu 2023, Samonte 2023, dsb.) menitikberatkan peningkatan literasi umum atau pengenalan risiko siber, tanpa fokus pada isu ransomware tertentu.

Hingga saat ini belum ada penelitian yang menilai literasi mahasiswa terhadap serangan ransomware pada infrastruktur penting seperti Pusat Data Nasional. Padahal, kasus PDNS 2024 menunjukkan potensi kerugian besar bila infrastruktur digital kritis terekspos [8]. Oleh karena itu, penelitian "Pengetahuan Mahasiswa Mengenai Isu Keamanan Sekuriti pada Pusat Data Nasional: Ransomware" mengisi gap literatur tersebut. Penelitian ini akan melengkapi temuan sebelumnya dengan memetakan pemahaman mahasiswa tentang ransomware dan ancaman terkait, sehingga menghadirkan kontribusi kebaruan dalam kajian keamanan siber kampus.

III. METODE PENELITIAN

Penelitian ini bertujuan untuk mengevaluasi pengetahuan mahasiswa mengenai isu keamanan sekuriti pada Pusat Data Nasional, khususnya mengenai ancaman ransomware, melalui pendekatan edukatif berbasis webinar. Metode penelitian yang digunakan meliputi beberapa tahapan, yaitu:

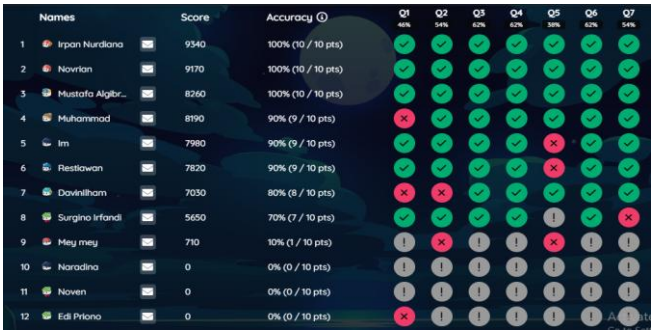
A. Webinar Series

Webinar series dirancang untuk memberikan pemahaman mendalam tentang isu keamanan sekuriti pada Pusat Data Nasional. Di Universitas Negeri Makassar, ditemukan bahwa literasi digital mendukung pembelajaran mandiri mahasiswa secara signifikan [17]. Materi webinar mencakup topik-topik seperti pengenalan dasar keamanan siber, teknik perlindungan terhadap ransomware, dan studi kasus serangan

ransomware pada infrastruktur penting. Webinar dilakukan secara daring selama 2 jam. Setiap sesi diisi oleh pakar di bidang cyber security dan diikuti dengan sesi tanya jawab untuk memperdalam pemahaman peserta.

B. *Pre-Test*

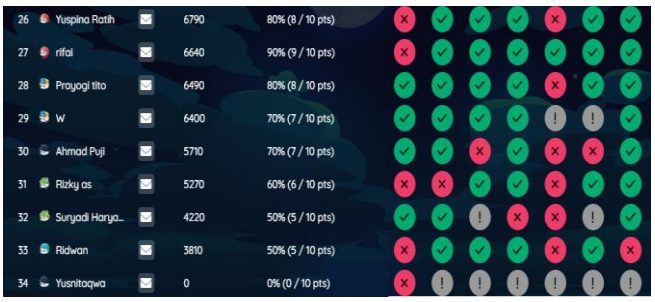
Sebelum dimulainya *webinar series*, mahasiswa yang menjadi peserta diminta untuk mengikuti *pre-test*. *Pre-test* ini bertujuan untuk mengukur tingkat pemahaman awal mahasiswa tentang isu keamanan siber, khususnya mengenai ancaman ransomware. Soal *pre-test* dirancang untuk mengevaluasi pengetahuan konseptual dan praktis mengenai teknik-teknik dasar keamanan siber. Gambar 1 menunjukkan pengambilan pre-test dengan menggunakan media quizzes.



Gambar 1. Hasil Pre-Test

C. *Post-Test*

Setelah mengikuti seluruh rangkaian webinar, mahasiswa diwajibkan mengikuti *post-test* yang sama dengan pre-test. Post-test ini bertujuan untuk mengukur peningkatan pengetahuan dan pemahaman mahasiswa setelah mengikuti webinar series. Hasil dari pre-test dan *post-test* akan dibandingkan untuk menilai efektivitas dari webinar dalam meningkatkan pengetahuan mahasiswa mengenai keamanan siber. Gambar 2 menunjukkan pengambilan *pre-test* dengan menggunakan media quizzes.



Gambar 2. Hasil Post-Test

D. *Sampel Penelitian*

Sampel penelitian ini terdiri dari mahasiswa program studi informatika dari Universitas Islam Mulia Yogyakarta dan Universitas Siber Muhammadiyah (Sibermu). Pemilihan sampel dilakukan secara acak dari mahasiswa yang telah menyatakan minat untuk berpartisipasi dalam webinar series. Total peserta yang terlibat dalam penelitian ini adalah 50 mahasiswa, dengan distribusi yang seimbang dari kedua universitas.

E. *Analisis Kuantitatif terhadap Efektivitas Edukasi Keamanan Siber*

Data yang diperoleh dari pre-test dan post-test dianalisis secara kuantitatif untuk mengidentifikasi perubahan signifikan dalam pengetahuan mahasiswa. Analisis dilakukan menggunakan uji t berpasangan (paired sample t-test) untuk membandingkan rata-rata skor sebelum dan sesudah mengikuti webinar. Uji normalitas Shapiro-Wilk diterapkan pada selisih skor untuk memastikan terpenuhinya asumsi distribusi normal. Selain itu, dihitung Cohen's d untuk menentukan besar pengaruh (effect size) dari intervensi. Seluruh analisis dilaksanakan dengan bantuan perangkat lunak statistik Python dengan tingkat signifikansi $\alpha = 0{,}05$.

Analisis statistik digunakan untuk menilai efektivitas webinar sebagai metode edukasi dalam meningkatkan kesadaran dan pemahaman mahasiswa tentang ancaman siber, khususnya *ransomware*. Hasil analisis ini diharapkan dapat memberikan gambaran mengenai strategi edukasi yang efektif dalam meningkatkan literasi keamanan siber di kalangan mahasiswa.

IV. HASIL DAN PEMBAHASAB

Penelitian ini melibatkan 50 koresponden dari mahasiswa program studi informatika yang mengikuti webinar series mengenai keamanan siber dan ancaman ransomware. Responden yang mengikuti pre-test dan post-test terdiri dari 7 soal. Analisis data dilakukan dengan membandingkan hasil pre-test dan post-test untuk mengukur peningkatan pengetahuan mahasiswa setelah mengikuti webinar.

A. *Hasil Analisis Deskriptif*

Hasil pre-test menunjukkan nilai rata-rata sebesar 52,50 dengan simpangan baku 18,91, nilai tertinggi 100 (3 responden), dan nilai terendah 0 (3 responden). Hasil post-test menunjukkan nilai rata-rata sebesar 85,30 dengan simpangan baku 15,05, nilai tertinggi 100 (11 responden), dan nilai terendah 0 (1 responden). Tabel 1 menunjukkan Statistik Deskriptif Pre-Test dan Post-Test.

TABEL I. STATISTIK DESKRIPTIF PRE-TEST DAN POST-TEST

Variabel	Mean	Median	SD	Min	Max	Perfect (100)	Zero (0)
Pre-Test	52,50	52,50	18,91	0	100	3	3
Post-Test	85,30	85,65	15,05	0	100	11	1

Peningkatan rata-rata skor sebesar 32,80 poin menunjukkan adanya perbaikan signifikan dalam pengetahuan mahasiswa setelah mengikuti pembelajaran.

B. *Metode Statistik*

Untuk menguji perbedaan skor pre-test dan post-test, digunakan paired-samples t-test. Sebelum uji t dijalankan, normalitas distribusi selisih skor diperiksa menggunakan Shapiro–Wilk test, dengan hasil $p < 0{,}05$ yang mengindikasikan data tidak berdistribusi normal. Oleh karena

itu, sebagai uji konfirmasi digunakan Wilcoxon signed-rank test.

Ukuran efek dihitung menggunakan Cohen's d untuk data berpasangan, dengan nilai d = 1,35 yang termasuk kategori efek besar.

C. *Hasil Uji Hipotesis*

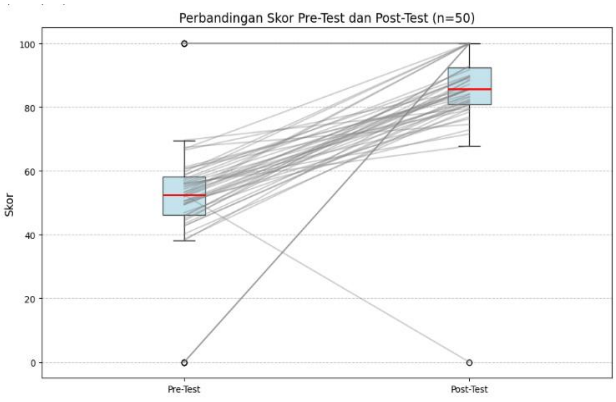
Hasil paired-samples t-test menunjukkan perbedaan signifikan antara skor pre-test dan post-test ($t(49) = 9{,}55$; $p < 0{,}001$). Hasil Wilcoxon signed-rank test juga menunjukkan perbedaan signifikan ($p < 0{,}001$), memperkuat temuan bahwa terjadi peningkatan pengetahuan yang bermakna setelah intervensi pembelajaran.

D. *Diskusi dan Interpretasi*

Hasil analisis menunjukkan adanya peningkatan skor yang besar dan signifikan antara pre-test dan post-test. Nilai rata-rata post-test yang lebih tinggi (85,30) dibandingkan pre-test (52,50) mengindikasikan bahwa intervensi pembelajaran yang diberikan berhasil meningkatkan pemahaman responden terhadap materi yang diujikan.

Ukuran efek yang tinggi (Cohen's d = 1,35) memperkuat temuan bahwa perbedaan ini tidak hanya signifikan secara statistik, tetapi juga memiliki makna praktis yang besar. Dengan kata lain, perubahan skor bukan sekadar akibat kebetulan, melainkan mencerminkan peningkatan kemampuan yang substansial.

Hasil uji normalitas menunjukkan bahwa distribusi selisih skor pre–post tidak berdistribusi normal, yang menandakan adanya variasi respons antar peserta — beberapa mengalami peningkatan yang sangat besar, sementara sebagian lainnya mengalami peningkatan moderat. Meski demikian, konsistensi hasil antara paired-samples t-test dan Wilcoxon signed-rank test membuktikan bahwa temuan ini cukup robust terhadap pelanggaran asumsi normalitas. Gambar 3 menunjukkan perbandingan pre-test dan post-test per peserta.



Gambar 3. Grafik perbandingan pre-test dan post-test

Temuan ini sejalan dengan literatur yang menyatakan bahwa intervensi terstruktur dengan metode pembelajaran aktif dapat memberikan dampak signifikan terhadap peningkatan hasil belajar. Dalam konteks ini, peningkatan pengetahuan mahasiswa mendukung bahwa pembelajaran berbasis webinar dapat menjadi alternatif efektif dalam pendidikan keamanan siber.

Sejalan dengan temuan sebelumnya, strategi edukatif yang interaktif dan kontekstual mampu meningkatkan kesadaran serta keterlibatan peserta dalam topik kritis seperti keamanan informasi [5]. Webinar yang dirancang dengan melibatkan praktisi, studi kasus nyata, dan sesi tanya jawab terbukti mendorong keterlibatan aktif mahasiswa [5]. Partisipasi aktif tersebut selaras dengan prinsip constructivist learning, di mana pemahaman dibentuk melalui pengalaman langsung dan interaksi bermakna [1].

Lebih lanjut, peningkatan pengetahuan ini juga menegaskan urgensi untuk memasukkan literasi keamanan siber ke dalam kurikulum pendidikan tinggi, terutama pada program studi yang berkaitan dengan teknologi informasi. Upaya ini penting untuk mempersiapkan generasi muda menghadapi ancaman siber yang semakin kompleks dan merusak [1][4][7].

V. KESIMPULAN

Penelitian ini membuktikan bahwa pendekatan edukatif berbasis webinar dapat secara signifikan meningkatkan pengetahuan mahasiswa mengenai isu keamanan siber, khususnya ancaman ransomware pada Pusat Data Nasional. Terjadi peningkatan rata-rata nilai sebesar 32,8 poin, dari 52,5 pada pre-test menjadi 85,3 pada post-test. Sebanyak 34 dari 50 mahasiswa mengalami peningkatan nilai, dan 11 mahasiswa mencapai skor sempurna.

Temuan ini memperkuat argumen bahwa strategi pembelajaran interaktif yang melibatkan praktisi dan studi kasus nyata dapat mempercepat pemahaman mahasiswa terhadap topik-topik keamanan digital yang kompleks. Selain itu, partisipasi aktif mahasiswa dalam diskusi juga menjadi faktor penting dalam keberhasilan proses pembelajaran.

Sebagai rekomendasi, penelitian ini menyarankan agar:

- Materi literasi keamanan siber diintegrasikan secara sistematis dalam kurikulum pendidikan tinggi, khususnya pada program studi teknologi informasi.
- Webinar dan pelatihan daring serupa diselenggarakan secara berkala sebagai bagian dari upaya peningkatan kesadaran dan ketahanan digital di kalangan mahasiswa.

Dengan membekali mahasiswa sejak dini dengan pemahaman tentang keamanan siber, Indonesia dapat lebih siap menghadapi tantangan era digital dan memperkuat pertahanan siber nasional.

DAFTAR PUSTAKA

[1] Badan Siber dan Sandi Negara (BSSN). (2021). *BSSN dorong pengembangan pusat data dalam negeri*. ANTARA News.

[2] Christmartha, M., Gultom, R. A. G., Aritonang, S., & Pertahanan, U. (2020). Strategi Kebijakan Pengembangan Sumber Daya Manusia Siber Nasional Guna Mendukung Pertahanan Negara the Policy Strategy of National Cybersecurity Human Resources Development To Support the National Defense (a Case Study At the National Cyber and Crypto Ag. *Jurnal Manajemen Pertahanan*, *6*(2), 85. https://www.cnnindonesia.com/teknol

[3] Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers and Security*, *79*, 162–189. https://doi.org/10.1016/j.cose.2018.08.008

[4] Düşmez, A. (2025). *Cyber information security awareness of university students (Central Anatolia region example)*. *4*(1), 126–137. https://doi.org/10.58583/EM.4.1.11

[5] Garba, A., Sirat, M., & Othman, S. (2021). Cybersecurity Awareness of University Students in Nigeria: Analysis Approach. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*, 3739–3752.

[6] IMF. (2024). *Chapter 3 Cyber Risk: A Growing Concern for Macrofinancial Stability*. 3.

[7] Jasmine, N., Nafilah, A., & Rahmadanti, R. (2025). Peran Mahasiswa Dalam Meningkatkan Kesadaran Keamanan Siber Di Lingkungan Kampus. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*, 109–121. https://doi.org/10.63217/fibonacci.v1i2.76

[8] Kementerian Komunikasi dan Informatika Republik Indonesia. (2019). *Apresiasi Siber Kreasi, Menkominfo Ingatkan Pentingnya Literasi Digital*.

[9] Nurul Fauziah Amri, Rosalyn Anwar, C., & Monoarfa, M. (2024). Analisis Literasi Digital Dalam Pembelajaran Mahasiswa Angkatan 2021 Prodi Teknologi Pendidikan Fakultas Ilmu Pendidikan Universitas Negeri Makassar. *Jurnal Teknologi Pendidikan*, *4*(2), 16–25. https://doi.org/10.37304/jtekpend.v4i2.14404

[10] Peker, Y. K., Ray, L., & Da Silva, S. (2018). Online cybersecurity awareness modules for college and high school students. *Proceedings - 2018 National Cyber Summit Research Track, NCS 2018*, *June 2018*, 24–33. https://doi.org/10.1109/NCS.2018.00009

[11] Puspita D, R. A. (2025). Analisis Ancaman Serangan Siber Pada Infrastruktur Informasi Vital Terhadap Stabilitas Keamanan Nasional. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *10*(5), 5397–5406. https://doi.org/10.36418/syntax-literate.v10i5.59084

[12] Riyadi, U. S. (2023). *PELATIHAN LITERASI KEAMANAN DIGITAL DI LINGKUNGAN UNIVERSITAS SLAMET RIYADI Lukas*. *7*(1), 45–50.

[13] Surdjono, H. D., Fadli, R., Sari, R. C., Eliza, F., Yassin, A., Kulanthaivel, G., Ramadhan, M. A., Mukhaiyar, R., Hamid, M. A., Ridwan, M. R., Purnomo, S., & Asnimawati. (2025). Effectiveness of Cybersecurity Awareness Program Based on Mobile Learning to Improve Cyber Hygiene. *International Journal of Information and Education Technology*, *15*(2), 220–229. https://doi.org/10.18178/ijiet.2025.15.2.2235

[14] Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam. *Jurnal Teknologi Dan Informasi*, *14*(2), 163–173. https://doi.org/10.34010/jati.v14i2.12518

[15] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004