E-ISSN: 2964-3171
P-ISSN: 2985-3214

JUPITER Volume 03 Nomor 01 Januari 2025

Pengaruh Hipersekuritisasi dan Praktik Keamanan Siber Harian Terhadap Kepatuhan Mahasiswa dalam Menghadapi Ancaman Digital

[1*]Muh Fikri Ainul Yakin, [2]Izulhak Algi Fahrizal, [3]Hajar Dewantara, Andi Naila Quin Azisah [4]Alisyahbana, [5]Salim Diarra

[1,2,3] Universitas Negeri Makassar
[4] Universitas Patompo
[5] Institut of Management and Language Applied to Business

Email: pampank79@gmail.com[1], algifahrizal01012002@gmail.com[2], hajardewantara@unm.ac.id[3], andinaila@unpatompo.ac.id[4] , salimdiarra@gmail.com
*Corresponding author: pampank79@gmail.com

Received : 15 Desember 2024
Accepted : 25 Januari 2025
Published : 31 Januari 2025

ABSTRAK

Meskipun kemajuan teknologi informasi memiliki banyak manfaat, mereka juga meningkatkan risiko keamanan siber, terutama bagi siswa. Tujuan penelitian ini adalah untuk melihat bagaimana hipersekuritisasi dan praktik keamanan siber harian mempengaruhi kepatuhan siswa terhadap kebijakan keamanan digital. Studi kuantitatif deskriptif ini melibatkan 94 siswa dari berbagai jurusan, dan data dikumpulkan melalui survei online yang menggunakan skala Likert lima tingkat. Hasil penelitian menunjukkan bahwa hipersekuritisasi memiliki nilai rata-rata 4,04, yang menunjukkan bahwa orang sangat waspada terhadap ancaman siber. Nilai rata-rata 4,01 untuk praktik keamanan siber harian menunjukkan perilaku positif seperti penggunaan autentikasi dua faktor dan pembaruan perangkat. Meskipun kebijakan yang lebih fleksibel diperlukan, nilai rata-rata 3,86 menunjukkan penerimaan kebijakan keamanan siber yang cukup tinggi. Studi ini menemukan bahwa untuk meningkatkan pengetahuan dan kepatuhan siswa tentang keamanan siber, metode berbasis pendidikan dan kebijakan yang lebih inklusif diperlukan.

Kata Kunci: Ancaman Digital, Hipersekuritisasi, Keamanan Siber, Kebijakan Keamanan Digital, Kepatuhan Siswa

ABTRACT

While advances in information technology have many benefits, they also increase cybersecurity risks, especially for students. The purpose of this study was to see how hypersecuritization and daily cybersecurity practices affect students' compliance with digital security policies. This descriptive quantitative study involved 94 students from various majors, and data was collected through an online survey that used a five-level Likert scale. The results showed that hypersecuritization had a mean score of 4.04, which indicates that people are very wary of cyber threats. The mean score of 4.01 for daily cybersecurity practices indicates positive behaviors such as the use of two-factor authentication and device updates. Although more flexible policies are needed, the mean score of 3.86 indicates a fairly high acceptance of cybersecurity policies. This study found that to improve students' knowledge and compliance about cybersecurity, education-based methods and more inclusive policies are needed.

Keywords: Digital Threats, Hypersecuritization, Cyber Security, Digital Security Policy, Student Compliance

This is an open access article under the CC BY-SA license

E-ISSN: 2985-3214
P-ISSN: 2964-3171

JUPITER Volume 03 Nomor 01 Januari 2025

1. PENDAHULUAN

Meskipun kemajuan teknologi informasi telah membawa banyak manfaat bagi masyarakat, juga membawa tantangan baru, terutama dalam hal keamanan siber. Berbagai kelompok, termasuk mahasiswa, sering kali menjadi sasaran ancaman digital di lanskap digital yang terus berubah. Ini adalah hasil dari peningkatan ketergantungan mereka pada teknologi dan kurangnya kesadaran keamanan siber (Gehrmann & Gunnarsson, 2020). Ancaman ini semakin relevan karena dunia digital menghadapi tren peningkatan serangan yang semakin canggih, seperti yang dilaporkan oleh banyak studi (Gehrmann & Gunnarsson, 2020). Hipersekuritisasi, sebuah tingkat pengamanan yang berlebihan yang dapat membatasi kebebasan pengguna tetapi tidak selalu efektif dalam mencegah serangan siber, adalah ancaman yang semakin kompleks seiring dengan perkembangan ancaman ini (Zermi, et al., 2021).

Banyak penelitian telah menunjukkan bahwa pendidikan dan kesadaran keamanan siber sangat penting untuk membuat dunia digital lebih aman. Menggabungkan strategi keamanan personal modern dengan teknologi enkripsi dapat menjadi solusi yang bertahan lama (Tijan et al., 2021). Di sisi lain,menekankan bahwa institusi sangat penting dalam mengajarkan keamanan kepada penggunanya, terutama mahasiswa, yang seringkali tidak memahami kompleksitas ancaman digital (Paul et al., 2023; Shrestha et al., 2020).

Meskipun hipersekuritisasi telah mendorong siswa untuk mematuhi kebijakan keamanan digital, hal ini juga dapat menyebabkan mereka terlalu bergantung pada sistem otomatis dan tidak memahami ancaman itu sendiri (Almeaibed et al., 2020; Lee et al., 2020). Menariknya, beberapa penelitian menunjukkan bahwa pendekatan yang didasarkan pada kerja sama antara lembaga pendidikan dan industri teknologi dapat meningkatkan keseimbangan antara fleksibilitas dan pengamanan pengguna (Ha, 2022). Selain itu, pemanfaatan teknologi berbasis manusia dalam pendekatan keamanan dapat membantu menciptakan lingkungan digital yang lebih inklusif (Atalay & Angin, 2020).

Namun, penelitian sebelumnya belum sepenuhnya membahas bagaimana kombinasi hipersekuritisasi dan praktik keamanan siber harian dapat memengaruhi kepatuhan akademik mahasiswa secara keseluruhan. Banyak penelitian saat ini hanya berkonsentrasi pada satu aspek, seperti dampak hipersekuritisasi atau praktik keamanan siber secara terpisah, tanpa mempertimbangkan bagaimana keduanya berpengaruh satu sama lain. Selain itu, studi sebelumnya tidak memberikan perhatian yang cukup pada kebutuhan siswa dan bagaimana mereka melihat diri mereka sebagai pengguna akhir kebijakan keamanan digital (Zermi et al., 2021; Dedkova et al., 2022).

Penelitian ini membantu dengan menawarkan metode yang lebih menyeluruh untuk mengevaluasi dampak gabungan dari hipersekuritisasi dan praktik keamanan harian terhadap kepatuhan siswa. Selain itu, temuan penelitian ini memberikan dasar untuk pembuatan kebijakan keamanan digital yang lebih terbuka dan sesuai dengan kebutuhan pengguna di institusi pendidikan tinggi.

Metode berbasis risiko, seperti simulasi digital twin, pelatihan interaktif, dan penyediaan materi pembelajaran berbasis teknologi, dapat digunakan untuk meningkatkan kesadaran keamanan siber siswa (Ross et al., 2020). Selain itu, pendekatan berbasis risiko, seperti simulasi ancaman, dapat membantu menemukan masalah keamanan dalam sistem Pendidikan (Aldughayfiq & Sampalli, 2021; Hadar et al., 2020).

Tujuan dari penelitian ini adalah untuk mempelajari lebih lanjut tentang bagaimana hipersekuritisasi dan praktik keamanan siber harian memengaruhi tingkat kepatuhan siswa terhadap ancaman digital. Dengan menggunakan penelitian sebelumnya, artikel ini akan memberikan perspektif teoretis dan saran praktis tentang cara institusi pendidikan dapat meningkatkan strategi keamanan digital mereka.

E-ISSN: 2985-3214
P-ISSN: 2964-3171
JUPITER Volume 03 Nomor 01 Januari 2025

2. METODE PENELITIAN

Penelitian kuantitatif deskriptif ini bertujuan untuk menunjukkan bagaimana praktik keamanan siber harian dan hipersekuritisasi berdampak pada kepatuhan mahasiswa terhadap kebijakan keamanan siber. Sesuai dengan rekomendasi literatur terkait, desain deskriptif digunakan untuk memaparkan data secara sistematis tanpa memeriksa hubungan kausal antarvariabel (Zermi et al., 2021). Desain ini banyak digunakan dalam penelitian keamanan siber karena kemampuannya memberikan wawasan awal tentang persepsi dan perilaku individu terhadap ancaman digital (Zermi et al., 2021; Almeaibed et al., 2021).

Populasi penelitian terdiri dari mahasiswa universitas negeri yang aktif dari berbagai jurusan dan metode pengambilan sampel non-probability dengan pendekatan convenience digunakan. Meskipun metode ini tidak sepenuhnya representatif, ia memungkinkan pengumpulan data yang efektif (Isaac et al., 2022). Metode ini sering digunakan dalam penelitian pendidikan tinggi karena fleksibilitasnya dan kemudahan implementasinya (Bhujel & Rahulamathavan, 2022; Marelli, 2020).

Data dikumpulkan melalui survei yang disebarkan secara online dari Oktober hingga November 2024. Kuesioner dibuat menggunakan skala Likert yang terdiri dari lima tingkatan, masing-masing menunjukkan tingkat ketidaksepakatan penuh dari 1 hingga 5. Metode yang disarankan dalam penelitian serupa menunjukkan bahwa metode ini dipilih untuk meningkatkan kecepatan pengumpulan data dan mempermudah akses responden (Tijan et al., 2021; Shrestha et al., 2020). Skala Likert telah terbukti efektif dalam mengukur persepsi individu terhadap variabel yang kompleks seperti keamanan siber (Yasin dkk, 2023).

Instrumen penelitian ini mencakup tiga variabel utama:

1. Hipersekuritisasi dalam Keamanan Siber, yang mengukur persepsi responden tentang ancaman siber yang dianggap penting di lingkungan pendidikan.
2. Praktik Keamanan Siber Harian oleh Mahasiswa, yang mengevaluasi tindakan responden dalam menjaga keamanan digital sehari-hari.
3. Kepatuhan Mahasiswa terhadap Kebijakan Keamanan Siber, yang menilai sejauh mana mahasiswa mengikuti aturan dan kebijakan keamanan digital.

Lima pernyataan untuk setiap variabel dibuat berdasarkan literatur yang relevan dan telah divalidasi oleh pakar keamanan siber untuk memastikan instrumen penelitian benar dan sah (Wang et al., 2024).

Statistik deskriptif digunakan untuk menganalisis data yang diperoleh. Untuk setiap item dalam kuesioner, analisis ini mencakup perhitungan modus, median, dan rata-rata (mean). Selain itu, distribusi frekuensi responden pada setiap kategori skala Likert dianalisis untuk memberikan gambaran umum tentang pola respons siswa terhadap hipersekuritisasi, praktik keamanan harian, dan tingkat kepatuhan terhadap kebijakan keamanan siber (Paul et al., 2023). Analisis ini memberikan dasar yang kuat untuk memahami tren perilaku mahasiswa dalam konteks ancaman digital (Sahi et al., 2022; Joshi et al., 2021).

Tabel 1. Kisi-kisi Instrumen

No	Aspek / Sub Faktor	Pernyataan	Nomor Pernyataan	Referensi
1	Hipersekuritisasi dalam Keamanan Siber	Saya sering mendengar ancaman siber disampaikan sebagai risiko besar yang memerlukan perhatian segera.	1	[22]
		Media sering menekankan potensi ancaman siber yang dapat berdampak serius pada kehidupan kita.	2	
		Saya percaya bahwa ancaman siber dianggap sebagai isu keamanan penting di lingkungan pendidikan	3	
		Saya merasa adanya urgensi dalam menghadapi ancaman siber di berbagai sektor, termasuk kampus.	4	

E-ISSN: 2985-3214
P-ISSN: 2964-3171
JUPITER Volume 03 Nomor 01 Januari 2025

		Informasi tentang ancaman siber yang saya terima cenderung menekankan risiko yang signifikan.	5
2	Praktik Keamanan Siber Harian oleh Mahasiswa	Saya secara rutin memperbarui kata sandi untuk menjaga keamanan akun-akun online	1
		Saya selalu waspada ketika membuka file dari sumber yang tidak dikenal.	2
		Saya berhati-hati saat menggunakan Wi-Fi publik di area kampus.	3
		Saya menggunakan autentikasi dua faktor untuk melindungi akun-akun saya.	4
		Saya memastikan perangkat saya diperbarui secara berkala untuk keamanan.	5
3	Kepatuhan Mahasiswa terhadap Kebijakan Keamanan Siber	Saya mengikuti kebijakan keamanan digital yang diberlakukan di kampus.	1
		Saya merasa penting untuk mematuhi aturan keamanan siber dalam aktivitas kampus sehari-hari.	2
		Saya mendukung kebijakan yang diterapkan untuk melindungi data dan privasi mahasiswa.	3
		Saya merasa wajib untuk menjaga keamanan data pribadi dan mengikuti protokol keamanan.	4
		Saya menyadari pentingnya protokol keamanan yang telah ditetapkan oleh institusi.	5

Tabel 2. Skala Likert

Skala	Jumlah Siswa
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Setuju

Setelah nilai rata rata maka jawaban telah diketahui, kemudian hasil tersebut diinterpretasikan berdasarkan Tabel 1 kemudian peneliti membuat garis kontinum:

$$\text{NJI (Nilai Jenjang Interval)} = \frac{Nilai\ Maks - Nilai\ Min}{Jumlah\ Kriteria\ Pernyataan} = \frac{5-1}{5-1} = 1$$

Tabel 3. Interval Skala Likert

Skala	Jumlah Siswa
1,00 – 1,75	Sangat Tidak Baik
1,76 – 2,50	Tidak Baik
2,51 – 3,25	Netral
3,26 – 4,00	Baik
4,01 – 5,00	Sangat Baik

3. HASIL DAN PEMBAHASAN

Penelitian ini melibatkan 94 responden mahasiswa yang mayoritas berasal dari kelompok jurusan STIEM sebanyak 81 Mahasiswa (Ilmu, Teknologi, Teknik, Informatika, dan Matematika) dan 12 Mahasiswa yang berasa dari Non - STIEM dan 1 Mahasiwa yang tidak mengisi dengan benar jurusan yang telah disediakan. Untuk menjaga integritas data, responden tidak menunjukkan jurusannya atau memberikan data yang tidak relevan. Oleh karena itu, data tersebut tetap dimasukkan dalam analisis. Berdasarkan data demografis, responden terdiri atas 48.9% laki-laki dan 51.1% perempuan, dengan rentang usia 17–21 tahun dan rata-rata usia 20,5 tahun. Sebagian besar responden menunjukkan kesadaran yang cukup tinggi terhadap isu keamanan siber dalam lingkungan pendidikan.

Tabel 4. Frequencies Jurusan

Jurusan	Counts	% of Total	Cumulative %
STEM	81	87.1 %	87.1 %
NON STEM	12	12.9 %	100.0 %

Tabel 5. Demograsi Responden

Gender	N	Percentage (%)	Mean age (years)
Male	46	48.9%	19.3
Female	48	51.1%	19.5
Total	94	100.0%	19.4

Tabel 6. Deskriptives Gender

	Jenis Kelamin
N	94

Tabel 7. Distribusi Responden Berdasarkan Gender

Jenis Kelamin	Counts	% of Total	Cumulative %
Perempuan	48	51.1 %	51.1 %
Laki-Laki	46	48.9%	100.0 %

Tabel 8. Descriptives Umur

	Umur laki-laki	Umur Perempuan
Mean	19.3	19.5

Tabel 9. Deskriptif Compute Total Umur Laki-Laki dan Perempuan

	Total keduanya
Mean	19.4

Tabel 9 diatas menunjukkan statistik deskriptif dari variabel Hipersekuritisasi dalam Keamanan Siber (V1), yang mengukur bagaimana mahasiswa melihat ancaman siber di lingkungan pendidikan. Nilai rata-rata untuk setiap subvariabel berkisar antara 3.91 dan 4.16, menunjukkan bahwa sebagian besar siswa sangat menyadari ancaman siber. Subvariabel v1 memiliki nilai rata-rata tertinggi, 4.16, menunjukkan bahwa mayoritas siswa melihat ancaman siber sebagai risiko yang serius yang membutuhkan perhatian segera. Ini sesuai dengan temuan Wang et al., 2024) yang menyatakan bahwa institusi pendidikan sering kali menggunakan pendekatan hipersekuritisasi untuk meningkatkan kesadaran terhadap ancaman siber. Namun, metode ini dapat membuat mereka bergantung pada sistem pengamanan yang ketat dan mengurangi pemahaman langsung tentang ancaman siber.

Sebagaimana tercermin dari sub-variabel v2 dan v3, sebagian besar siswa menganggap ancaman siber sebagai masalah yang sangat penting di lingkungan pendidikan. Penyelarasan kebijakan keamanan siber dengan kebutuhan pendidikan sangat penting untuk meningkatkan kinerja kebijakan (Zermin et al., 2021). Namun

demikian, nilai rata-rata pada sub-variabel v5 yang sedikit lebih rendah (3.91) menunjukkan bahwa siswa berbeda-beda dalam pandangan mereka tentang seberapa pentingnya penerapan kebijakan keamanan. Kebijakan yang terlalu ketat atau terlalu otomatis dapat menyebabkan ketidaknyamanan bagi mahasiswa, meskipun kesadaran akan ancaman siber yang tinggi (Dedkova et al., 2022).

Secara keseluruhan, Tabel 9 menunjukkan bahwa siswa sangat memperhatikan ancaman siber. Hasil ini menunjukkan bahwa mahasiswa cenderung lebih berkonsentrasi pada penerapan kebijakan yang meningkatkan kewaspadaan mereka terhadap ancaman siber. Namun, ada kemungkinan bahwa hipersekuritisasi dapat membuat pemahaman mereka tentang ancaman tersebut berkurang. Pelatihan interaktif seperti simulasi ancaman dapat membantu siswa mengurangi ketergantungan pada sistem pengamanan otomatis dan meningkatkan pemahaman mereka tentang ancaman yang lebih nyata dan berkembang (Yasin dkk, 2024).

Adaupun pada tabel 10, hasil analisis menunjukkan bahwa nilai rata-rata komputasi untuk variabel ini adalah 4,04 (SD = 0,79). Nilai ini mencerminkan bahwa mayoritas mahasiswa menganggap ancaman siber sebagai isu yang serius di lingkungan pendidikan mereka, dan mereka lebih cenderung untuk memperhatikan kebijakan yang diterapkan terkait masalah keamanan digital. Ini sejalan dengan teori yang mengatakan bahwa hipersekuritisasi dapat meningkatkan kesadaran tentang ancaman siber, meskipun ini seringkali menghasilkan ketergantungan pada sistem pengamanan yang ketat (Balasundram et al., 2023; Standards et al., 2020).

Tabel 10. Descriptives Variabel Hipersekuritisasi dalam Keamanan Siber (V1)

	V1	**V2**	**V3**	**V4**	**V5**
Mean	4.16	4.06	4.13	3.96	3.91
Sum	391	382	388	372	368

Tabel 11. Descriptives Total Komputasi Variabel Hipersekuritisasi dalam Keamanan Siber (V1)

	V1
Mean	4,04

Tabel 11 menunjukkan statistik deskriptif dari variabel Praktik Keamanan Siber Harian oleh Mahasiswa (V2), yang menilai bagaimana mahasiswa mempertahankan keamanan internet. Nilai, berdasarkan nilai rata-rata (mean), berkisar antara 3.67 dan 4.32, dengan subvariabel v7 memiliki nilai tertinggi, yaitu 4.32. Hal ini menunjukkan bahwa sebagian besar siswa telah mengambil tindakan yang lebih proaktif untuk melindungi data mereka, seperti menggunakan autentikasi dua faktor dan secara teratur melakukan pembaruan perangkat lunak. Studi lain menunjukkan bahwa orang yang lebih menyadari ancaman siber cenderung mengambil langkah-langkah perlindungan tambahan (Hadar et al., 2020; Marelli, 2020).

Subvariabel v6, di sisi lain, menerima nilai rata-rata terendah (3.67), meskipun masih berada dalam kategori yang baik. Ini menunjukkan bahwa meskipun sebagian besar siswa mahir dalam keamanan digital, hal-hal seperti pembaruan kata sandi masih perlu dilakukan dengan lebih sering. Hal ini sesuai dengan temuan yang menunjukkan bahwa hal-hal dasar seperti memperbarui kata sandi sering diabaikan meskipun penting untuk melindungi data akademik dan pribadi siswa. Dalam mengajarkan siswa kebiasaan keamanan digital, pendekatan yang lebih luas diperlukan. Pendekatan ini harus diterapkan dengan lebih sering untuk meningkatkan kesadaran siswa dan pengelolaan risiko (Aldughayfiq & Sampalli; 2021).

Nilai total (sum) untuk masing-masing subvariabel menunjukkan bahwa subvariabel v7 memiliki nilai akumulasi tertinggi (406), yang menunjukkan bahwa siswa lebih sering menggunakan kebiasaan keamanan yang lebih ketat. Hal ini menunjukkan bahwa, meskipun ada peningkatan kesadaran akan ancaman siber, masalah utama tetap ada dalam menerapkan kebiasaan keamanan dasar dalam kehidupan sehari-hari siswa (Tijan et al. 2021; Bhujel & Rahulamathavan, 2022).

Secara keseluruhan, tabel ini menunjukkan bahwa kebiasaan keamanan digital siswa secara umum baik; namun, ada area yang perlu diperbaiki, terutama dalam hal konsistensi dalam melakukan tindakan pencegahan dasar seperti pembaruan kata sandi. Akibatnya, pendekatan pendidikan yang lebih mendalam diperlukan untuk mendorong kebiasaan ini untuk menjadi lebih konsisten dalam kegiatan sehari-hari siswa (Zermi et al., 2021; Marelli, 2020).

E-ISSN: 2985-3214
P-ISSN: 2964-3171
JUPITER Volume 03 Nomor 01 Januari 2025

Adaupun pada tabel 12 itu menjelaskan nilai rata-rata untuk variabel Praktik Keamanan Siber Harian adalah 4,01, dengan standar deviasi 0,83. Hal ini menunjukkan bahwa sebagian besar peserta memiliki kebiasaan yang baik untuk menjaga keamanan digital mereka. Praktik yang dimaksud termasuk menggunakan autentikasi dua faktor, memperbarui kata sandi secara teratur, dan berhati-hati saat menggunakan jaringan Wi-Fi publik. Nilai rata-rata yang tinggi menunjukkan bahwa siswa secara aktif melindungi data pribadi mereka dalam kehidupan sehari-hari (Saugmann, 2020; Rudnichenko et al., 2021).

Tabel 12. Descriptives Variabel Praktik Keamanan Siber Harian oleh Mahasiswa (V2)

	v6	v7	v8	v9	v10
Mean	3,67	4,32	3,90	4,10	4,09
Sum	345	406	367	385	384

Tabel 13. Descriptives Total Komputasi Variabel Praktik Keamanan Siber Harian oleh Mahasiswa (V2)

	V2
Mean	4,01

Untuk memberikan gambaran tentang kepatuhan siswa terhadap kebijakan keamanan siber (V3), tabel 13 menggunakan statistik deskriptif untuk menunjukkan lima subvariabel yang mengukur tingkat kepatuhan siswa terhadap kebijakan keamanan siber. Ada perbedaan dalam tingkat kepatuhan siswa terhadap kebijakan tersebut, meskipun rata-rata (mean) nilai sub-variabel adalah 3.07–4.28.

Sub-variabel v14 menunjukkan nilai rata-rata tertinggi (4.28), yang menunjukkan bahwa mayoritas mahasiswa memiliki kesadaran dan kesiapan untuk mematuhi kebijakan yang diterapkan. Mereka cenderung merasa bahwa kebijakan ini sangat penting dalam menjaga keamanan siber di lingkungan kampus. Sebaliknya, sub-variabel v11 mencatatkan nilai rata-rata terendah (3.07), yang menunjukkan adanya tingkat kepatuhan yang lebih rendah pada kebijakan tertentu. Hal ini bisa disebabkan oleh berbagai faktor, termasuk kurangnya pemahaman tentang kebijakan yang ada atau kurangnya kejelasan dalam penerapannya. Penelitian oleh Sahi et al., (2022) menunjukkan bahwa faktor psikologis dan organisasi berperan besar dalam pengaruh kepatuhan terhadap kebijakan, dan bahwa pemahaman yang lebih baik akan kebijakan dapat meningkatkan tingkat kepatuhan mahasiswa.

Sikap siswa terhadap kebijakan keamanan siber sangat berbeda tergantung pada tingkat pendidikan mereka, siswa pascasarjana lebih cenderung mengikuti kebijakan daripada siswa sarjana, menurut data sub-variabel yang menunjukkan perbedaan tingkat kepatuhan antara kelompok siswa dalam penelitian tersebut (Torres & Gallego-Arrufat, 2022).

Selain itu, penelitian tentang persepsi dan perilaku siswa di tiga negara yang berbeda bahwa kondisi sosial, ekonomi, dan kebijakan pemerintah dasar seringkali memengaruhi kebijakan keamanan siber di perguruan tinggi. Kondisi eksternal ini memengaruhi seberapa baik siswa mematuhi kebijakan tersebut (Tijan et al., 2021).

Secara keseluruhan, Tabel 13 menunjukkan bahwa meskipun tingkat kepatuhan terhadap kebijakan keamanan siber cukup tinggi, sulit untuk memastikan bahwa semua siswa memahaminya. Faktor-faktor seperti pelatihan berkelanjutan dan komunikasi kebijakan yang lebih baik sangat penting untuk meningkatkan kepatuhan mahasiswa terhadap kebijakan tersebut. Sosialisasi dan pelatihan yang lebih terorganisir sangat penting untuk meningkatkan kepatuhan terhadap kebijakan keamanan di institusi pendidikan tinggi (Saugmann, 2020).

Pada tabel 14 itu menunjukkan nilai rata-rata untuk variabel Kepatuhan terhadap Kebijakan Keamanan Siber adalah 3,86, dengan standar deviasi 1,28. Meskipun angka ini menunjukkan bahwa banyak siswa mematuhi kebijakan kampus, variasi besar dalam respons menunjukkan bahwa meskipun banyak siswa mematuhi kebijakan, ada juga yang merasa kebijakan kurang relevan atau perlu diubah untuk memenuhi kebutuhan mereka (Dedkova et al., 2022; Coles-Kemp et al., 2020).

Tabel 14. Descriptives Variabel Kepatuhan Mahasiswa terhadap Kebijakan Keamanan Siber (V3)

	v11	**v12**	**v13**	**v15**	**v14**
Mean	3,07	3,69	4,03	4,21	4,28
Sum	89	107	117	122	124

Tabel 14. Descriptives Total Komputasi Variabel Kepatuhan Mahasiswa terhadap Kebijakan Keamanan Siber (V3)

	V3
Mean	3,86

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa mayoritas siswa menyadari ancaman siber dan praktik keamanan digital yang baik. Kebijakan keamanan siber yang diterapkan oleh kampus juga terbukti efektif dalam meningkatkan kepatuhan siswa terhadap aturan yang ada, meskipun beberapa siswa percaya bahwa kebijakan harus diubah agar lebih nyaman bagi pengguna.

Untuk menginterpretasikan temuan penelitian ini, ada beberapa keterbatasan. Pertama, hasil penelitian tidak dapat digeneralisasikan untuk seluruh populasi mahasiswa karena pengambilan sampel dilakukan dengan metode convenience sampling, yang merupakan metode non-probability sampling. Kedua, responden mungkin bias karena mengisi kuesioner dengan jujur atau tidak memahami pertanyaan. Selain itu, penelitian ini hanya berkonsentrasi pada dua variabel utama: hipersekuritisasi dan praktik keamanan siber harian. Tidak ada faktor eksternal lainnya yang dapat memengaruhi kepatuhan siswa, seperti dukungan institusi atau pengaruh sosial. Syarat terakhir adalah desain penelitian kuantitatif deskriptif yang digunakan. Ini menghalangi analisis hubungan kausal antarvariabel.

4. KESIMPULAN DAN SARAN

Studi ini menunjukkan bahwa hipersekuritisasi dan praktik keamanan siber harian memengaruhi kepatuhan siswa terhadap ancaman digital. Nilai rata-rata tinggi pada variabel ini menunjukkan bahwa sebagian besar siswa menyadari pentingnya keamanan digital. Mahasiswa mengadopsi praktik keamanan positif, seperti autentikasi dua faktor dan pembaruan perangkat lunak secara teratur. Namun, tingkat kepatuhan terhadap kebijakan keamanan digital masih berbeda, menunjukkan bahwa pendekatan yang lebih terbuka diperlukan. Penelitian ini sangat meningkatkan pemahaman kita tentang perilaku siswa terhadap ancaman siber dan kebijakan keamanan. Ini juga memberikan dasar bagi lembaga pendidikan untuk membuat strategi keamanan digital yang lebih baik.

Untuk meningkatkan kesadaran siswa terhadap ancaman siber dan meningkatkan literasi digital melalui program pendidikan yang lebih komprehensif, penelitian menunjukkan bahwa institusi pendidikan harus membuat kebijakan keamanan siber yang lebih fleksibel dan sesuai dengan kebutuhan siswa untuk meningkatkan tingkat kepatuhan siswa. Selain itu, simulasi ancaman dan teknik berbasis teknologi dapat digunakan untuk membantu siswa memahami risiko. Penelitian tambahan dapat dilakukan untuk mengetahui bagaimana dinamika sosial dan budaya organisasi memengaruhi kepatuhan terhadap kebijakan keamanan siber.

REFERENSI

Aldughayfiq, B., & Sampalli, S. (2021). Digital Health in Physicians' and Pharmacists' Office: A Comparative Study of e-Prescription Systems' Architecture and Digital Security in Eight Countries," *Omi. A J. Integr. Biol.*, 25(2) 102–122, doi: 10.1089/omi.2020.0085.

Almeaibed, S., Al-Rubaye, S., Tsourdos, A., & Avdelidis, N.P. (2021). Digital Twin Analysis to Promote Safety and Security in Autonomous Vehicles," *IEEE Commun. Stand. Mag.*, 5(1), 40–46, doi: 10.1109/MCOMSTD.011.2100004.

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

Balasundram, S.K., Shamshiri, R.R., Sridhara, S., & Rizan, N. (2023). The Role of Digital Agriculture in Mitigating Climate Change and Ensuring Food Security: An Overview. *Sustain.* 15(6), doi:

E-ISSN: 2985-3214
P-ISSN: 2964-3171

JUPITER Volume 03 Nomor 01 Januari 2025

10.3390/su15065325.

Bhujel, S., and Rahulamathavan, Y. (2022). A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces," *Sensors*, 22(22) doi: 10.3390/s22228833.

Coles-Kemp, L., Jensen, R.B., & Heath, C.P.R. (2020). Too Much Information: Questioning Security in a Post-Digital Society. *Conf. Hum. Factors Comput. Syst. - Proc.*, 1–14,, doi: 10.1145/3313831.3376214.

Dedkova L., Smahel D., and Just M. (2022). Digital security in families: the sources of information relate to the active mediation of internet safety and parental internet skills. *Behav. Inf. Technol.*, 41(5) 1052–1064, doi: 10.1080/0144929X.2020.1851769.

Gehrmann, C., & Gunnarsson, M. (2020). A digital twin based industrial automation and control system security architecture. *IEEE Trans.* Ind. Informatics, 16(1), 669–680. doi: 10.1109/TII.2019.2938885.

Ha L. T. (2022). Are digital business and digital public services a driver for better energy security? Evidence from a European sample. *Environ. Sci. Pollut. Res.*, 29(18), 27232–27256, doi: 10.1007/s11356-021-17843-2

Hadar, E., Kravchenko, & Basovskiy, A. (2020) Cyber Digital Twin Simulator for Automatic Gathering and Prioritization of Security Controls' Requirements. *Proc. IEEE Int. Conf. Requir. Eng.*, 250–259, doi: 10.1109/RE48521.2020.00035.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school," *Int. Stud. Q.* 53(4), 1155–1175, doi: 10.1111/j.1468-2478.2009.00572.x.

Isaac A.O., Alawida, M., Esther O.A, and Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *J. King Saud Univ. - Comput. Inf. Sci.*, 34(10), 10217–10245, doi: 10.1016/j.jksuci.2022.10.018.

Joshi, A.B., Kumar, D., & Mishra, D.C. (2021). Security of Digital Images Based on 3D Arnold Cat Map and Elliptic Curve. *Int. J. Image Graph.*, 21(1), doi: 10.1142/S0219467821500066.

Lee C., S., Han, M., & Seong, M.P. (2020). Development of a quantitative method for identifying fault-prone cyber security controls in NPP digital I&C systems. *Ann. Nucl. Energy*, Vol. 142, p. 107398, doi: 10.1016/j.anucene.2020.107398.

Marelli, M. (2020). Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation. *Int. Rev. Red Cross*, 102(913) 367–387, doi: 10.1017/S1816383121000151.

Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterp. Inf. Syst.*, 15(4) 565–584, doi: 10.1080/17517575.2019.1600041.

Paul M., L. Maglaras, Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 9(4), 571–588, doi: 10.1016/j.icte.2023.02.007.

Ross, A., Banerjee, S., & Chowdhury, A. (2020). Security in smart cities: A brief review of digital forensic schemes for biometric data. *Pattern Recognit. Lett.*, Vol. 138, 346–354, doi: 10.1016/j.patrec.2020.07.009.

Rudnichenko, Y., Melnyk, S., Havlovska, N., Illiashenko, O., & Nakonechna, N. (2021). Strategic interaction of state institutions and enterprises with economic security positions in digital economy. *WSEAS Trans. Bus. Econ.*. 18(1), 218–230, 2021, doi: 10.37394/23207.2021.18.23.

Sahi, A.M., Khalid, H., Abbas A.F., Zedan, F., Khatib S.F.A, and Al Amosh, H. (2022). The Research Trend of Security and Privacy in Digital Payment. *Informatics*, 9(2), doi: 10.3390/informatics9020032.

Saugmann, R. (2020). The security captor, captured. Digital cameras, visual politics and material semiotics. *Crit. Stud. Secur.* 8(2) 130–144, 2020, doi: 10.1080/21624887.2020.1815479.

E-ISSN: 2985-3214
P-ISSN: 2964-3171

JUPITER Volume 03 Nomor 01 Januari 2025

Shrestha, Wenan, T., Khadka, A., & Jeong, S.R.. (2020). Digital Tourism Security System for Nepal. KSII Trans. Internet Inf. Syst. 14(11), 4331–4354, doi: 10.3837/tiis.2020.11.005.

Standards, A. U. S. D., Stevens, R., Dykstra, J., Everette, W.K., & Chapman, J.(2020). Compliance Cautions : Investigating Security.

Tijan, E., Jović, S. Aksentijević, & A. Pucihar. (2021). Digital transformation in the maritime transport sector. *Technol. Forecast. Soc. Change*. 170(1), doi: 10.1016/j.techfore.2021.120879.

Torres, H.N., & Gallego-Arrufat, M.J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Educ. Inf. Technol.* 27(6) 8583–8602, doi: 10.1007/s10639-022-10978-w.

Wang, S., Jiang, X., and Khaskheli, M.B. (2024). The Role of Technology in the Digital Economy's Sustainable Development of Hainan Free Trade Port and Genetic Testing: Cloud Computing and Digital Law," *Sustain.*, 16(14), doi: 10.3390/su16146025.

Yasin, A., Fatima, R., JiangBin, Z., Afzal, W., and Raza, S. (2023). Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in Information Security. *Inf. Softw. Technol.* 170(1),107426, doi: 10.1016/j.infsof.2024.107426.

Zermi, N., Khaldi, A., Kafi, R., Kahlessenane, F., & Euschi, S. (2021). A DWT-SVD based robust digital watermarking for medical image security. Forensic Sci. Int., 320(1) doi: 10.1016/j.forsciint.2021.110691.