Jurnal Vocational Teknik Elektronika dan Informatika
http://ejournal.unp.ac.id/index.php/voteknika
Universitas Negeri Padang, Indonesia

ISSN 2302-3295 (Print)
ISSN 2716-3989 (Electronics)
Vol. 13, No. 4, 2025

Determinants of Cybersecurity Behavior among Social Media Users: The Moderating Role of *Self-efficacy* in the Relationship between Cybersecurity Knowledge and Social Media Use Intensity

Hadi Kurnia Saputra*[1], Refdinal[2], Rijal Abdullah[3], Jonni Mardizal[4], Ambiyar[5], Fadhilah[6]

[1,2,3,4,5,6]Universitas Negeri Padang, Padang, Padang, Indonesia

*Corresponding Author: hadiksaputra@ft.unp.ac.id

Abstract - ***Social media has become an integral part of daily life, but its intensive use also increases users' exposure to various cybersecurity threats, making it important to understand the determinants of cybersecurity behavior. This study examines the effects of cybersecurity knowledge and social media usage intensity on cybersecurity behavior, as well as the role of cybersecurity self-efficacy as both a direct predictor and a moderating variable. A quantitative approach was employed using a survey of 115 university students who actively use social media, and the data were analyzed using Structural Equation Modeling–Partial Least Squares (SEM-PLS). The results indicate that cybersecurity knowledge has a positive and significant effect on cybersecurity behavior (β = 0.309, t = 3.383, p < 0.01), while cybersecurity self-efficacy emerges as the strongest predictor of cybersecurity behavior (β = 0.479, t = 4.725, p < 0.001). In contrast, social media usage intensity does not show a significant effect on cybersecurity behavior (β = 0.003, t = 0.032, p > 0.05). Furthermore, moderation analysis reveals that cybersecurity self-efficacy does not moderate the relationships between cybersecurity knowledge or social media usage intensity and cybersecurity behavior. The structural model explains 58.3% of the variance in cybersecurity behavior (R^2 = 0.583). These findings suggest that cybersecurity behavior among social media users is more strongly driven by cognitive and psychological factors than by usage intensity alone. Practically, effective cybersecurity interventions should prioritize strengthening users' cybersecurity knowledge and self-efficacy rather than merely restricting social media use.***

Keywords— ***Cybersecurity behavior; Cybersecurity knowledge; Self-efficacy; Social media usage intensity; SEM-PLS***

I. PENDAHULUAN

Media sosial telah menjadi kanal utama interaksi digital bagi pengguna, mencakup komunikasi personal, pertukaran informasi, penyebaran konten, serta pembentukan identitas dan jejaring sosial [1], [2], [3], [4]. Seiring dengan meningkatnya intensitas penggunaan platform seperti Instagram, Facebook, TikTok, dan YouTube, pengguna juga menghadapi paparan yang semakin tinggi terhadap ancaman keamanan siber, termasuk *phishing*, pengambilalihan akun, penyalahgunaan data pribadi, dan rekayasa sosial yang mengeksploitasi pola perilaku *online*. Sejumlah studi menunjukkan bahwa intensitas penggunaan media sosial berpotensi meningkatkan risiko keamanan; namun, temuan empiris terkait pengaruh langsungnya terhadap perilaku keamanan siber masih menunjukkan hasil yang tidak konsisten [5], [6]. Di sisi lain, pengetahuan keamanan siber sering dianggap sebagai prasyarat penting dalam membentuk perilaku protektif, meskipun beberapa penelitian mengindikasikan bahwa tingkat pengetahuan yang memadai tidak selalu diikuti oleh penerapan praktik keamanan yang konsisten [7]. Ketidaksesuaian antara tingkat paparan risiko, pengetahuan keamanan, dan perilaku aktual pengguna ini menegaskan adanya celah penelitian terkait faktor psikologis internal yang menjembatani hubungan tersebut, khususnya peran *Self-efficacy* dalam membentuk dan memperkuat perilaku keamanan siber [8], [9].

Dalam konteks psikologi sosial dan pembentukan perilaku, *Social Cognitive Theory (SCT)* juga relevan karena menempatkan *Self-efficacy* sebagai determinan utama perilaku. SCT menekankan bahwa keyakinan individu terhadap kemampuan dirinya dalam melakukan tindakan tertentu secara langsung mempengaruhi konsistensi, intensitas, dan durabilitas perilaku tersebut. Penelitian yang diterbitkan dalam jurnal internasional memperlihatkan bahwa *Self-efficacy* berperan signifikan dalam praktek keamanan perangkat seperti smartphone, serta dalam menjelaskan variasi perilaku protektif di antara individu, bahkan ketika faktor teknis telah diakomodasi [10]. Selain itu, penelitian sistematis terkini menunjukkan pentingnya keandalan dan validitas *Self-efficacy* sebagai konstruk ketika mengukur perilaku keamanan siber, yang implikasinya sangat relevan bagi desain intervensi pendidikan atau sistem keamanan yang bertujuan meningkatkan perilaku pencegahan ancaman [10].

Tidak hanya faktor psikologis internal, intensitas penggunaan media sosial juga merupakan aspek penting ketika mengevaluasi perilaku keamanan siber. Intensitas ini mencerminkan frekuensi dan durasi interaksi pengguna dengan platform digital dan sering dioperasionalisasikan dalam studi perilaku sebagai indikator tingkat keterlibatan digital.

DOI: https://doi.org/10.24036/voteteknika.v13i4.137117
Received : 2025-12-25
Revised : 2025-12-28
Accepted : 2025-12-29
Published : 2025-12-30

Penelitian mengenai keterlibatan media sosial menyatakan bahwa intensitas penggunaan media sosial mencakup frekuensi akses, waktu penggunaan harian, dan keterikatan emosional pengguna terhadap *platform* tertentu, yang kemudian dapat mempengaruhi bagaimana risiko ancaman dipersepsikan dan direspons oleh pengguna [11]. Namun, intensitas tinggi tidak serta-merta menunjukkan perilaku keamanan yang baik; justru, paparan yang lebih sering terhadap konten digital dapat meningkatkan peluang terpapar konten atau tautan berisiko, sehingga keputusan perilaku protektif tetap bergantung pada tingkat pengetahuan dan keyakinan individu dalam menghadapi situasi berbahaya.

Pengetahuan keamanan siber merupakan determinan lain yang sering dikaitkan dengan perilaku protektif. Pengetahuan di sini mencakup pemahaman tentang jenis ancaman umum, langkah pencegahan yang efektif, serta implementasi praktik terbaik keamanan digital. Penelitian yang dilakukan pada pengguna digital banking di Indonesia menunjukkan bahwa pengetahuan keamanan memiliki pengaruh positif signifikan tidak hanya pada kesadaran tetapi juga perilaku keamanan, meskipun pengaruhnya terhadap mediasi kesadaran masih menjadi bahan diskusi metodologis dalam literatur [12]. Temuan semacam ini konsisten dengan studi lain yang menunjukkan bahwa individu dengan paparan pengetahuan yang tinggi cenderung lebih siap untuk menerapkan proteksi digital seperti penggunaan autentikasi dua faktor atau pembaruan perangkat lunak secara berkala.

Beberapa studi empiris yang relevan telah dilakukan dalam berbagai konteks demografis dan geografis. Sebuah studi di Ghana yang menggunakan integrasi PMT dan *Theory of Planned Behavior* (TPB) menunjukkan bahwa kesadaran keamanan siber dan persepsi ancaman secara signifikan memprediksi niat perilaku protektif pada mahasiswa, yang kemudian digunakan untuk merumuskan intervensi pendidikan yang kontekstual[13]. Selain itu, penelitian pada pengguna layanan perbankan digital menemukan bahwa pengetahuan memainkan peran dominan dalam memengaruhi perilaku keamanan, meskipun mediasi kesadaran tidak selalu signifikan, yang memberikan wawasan kontekstual penting mengenai bagaimana model empiris perlu disesuaikan dengan karakteristik populasi yang berbeda [12].

Di Indonesia, penelitian perilaku keamanan informasi semakin berkembang di lingkungan akademik dan profesional. Penelitian terbaru yang menganalisis *cybersecurity awareness* dan perilaku mahasiswa dengan integrasi PMT dan Theory of Planned Behavior menyimpulkan bahwa niat perilaku dan kesadaran memainkan peran signifikan dalam menjelaskan perilaku protektif mahasiswa, meskipun variabel seperti *Self-efficacy* dalam konteks tertentu tidak berpengaruh langsung pada niat [14]. Temuan ini menunjukkan bahwa meskipun model teoritis relatif konsisten, manifestasi empirisnya dapat bervariasi tergantung pada konteks budaya, tingkat literasi digital, dan karakteristik demografis populasi yang diteliti.

Mengacu pada temuan-temuan tersebut, terdapat kesenjangan riset (*research gap*) yang perlu dijawab. Pertama, studi yang menguji secara simultan pengaruh pengetahuan keamanan siber dan intensitas penggunaan media sosial terhadap perilaku keamanan siber pada konteks mahasiswa atau pengguna media sosial di Indonesia masih relatif sedikit, meskipun isu ini sangat dekat dengan aktivitas digital sehari-hari mahasiswa. Kedua, meskipun *Self-efficacy* sering diposisikan sebagai prediktor langsung dalam model perilaku, pengujian *Self-efficacy* sebagai variabel moderasi yaitu apakah ia memperkuat atau melemahkan hubungan antara pengetahuan dan intensitas penggunaan media sosial terhadap perilaku keamanan siber masih belum banyak dibahas secara spesifik dalam konteks pengguna media sosial. Padahal literatur menunjukkan *Self-efficacy* dapat berperan penting dalam memediasi atau menopang perilaku protektif, termasuk dalam menghadapi ancaman seperti phishing dan keputusan berbagi informasi yang sensitif [13].

Penelitian ini diharapkan memberikan kontribusi teoritis dan praktis, khususnya dalam konteks pendidikan tinggi di Indonesia, dengan membantu memahami kombinasi faktor kognitif (*knowledge*), perilaku digital (*intensity*), dan psikologis (*Self-efficacy*) yang berkaitan dengan perilaku protektif mahasiswa di lingkungan media sosial. Temuan yang dihasilkan diharapkan dapat dimanfaatkan sebagai dasar perancangan program literasi dan intervensi keamanan siber yang tidak hanya berfokus pada peningkatan pengetahuan teknis mahasiswa, tetapi juga pada penguatan keyakinan diri agar perilaku protektif dapat diterapkan secara lebih konsisten dalam menghadapi berbagai ancaman di era digital.

Penelitian ini bertujuan: (1) menganalisis pengaruh Pengetahuan Keamanan Siber (X1) terhadap Perilaku Keamanan Siber (Y); (2) menganalisis pengaruh Intensitas Penggunaan Media Sosial (X2) terhadap Perilaku Keamanan Siber (Y); (3) menganalisis pengaruh *Self-efficacy* Keamanan Siber (Z) terhadap Perilaku Keamanan Siber (Y); dan (4) menguji peran *Self-efficacy* sebagai moderator pada hubungan: (a) X1 → Y dan (b) X2 → Y.

II. METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan desain penelitian eksplanatori (*explanatory research*). Pendekatan ini dipilih untuk menjelaskan hubungan kausal antara variabel-variabel penelitian, yaitu Pengetahuan Keamanan Siber, Intensitas Penggunaan Media Sosial, *Self-efficacy* Keamanan Siber, dan Perilaku Keamanan Siber. Penelitian eksplanatori sesuai digunakan karena tujuan utama penelitian ini bukan hanya mendeskripsikan fenomena, tetapi menguji pengaruh langsung dan efek moderasi antar konstruk laten dalam suatu model struktural berbasis teori *Protection Motivation Theory* (PMT) dan *Social Cognitive Theory* (SCT).

Subjek penelitian adalah mahasiswa Universitas Negeri Padang yang aktif menggunakan media sosial. Mahasiswa dipilih sebagai subjek penelitian karena merupakan kelompok pengguna media sosial yang intensif serta memiliki risiko paparan ancaman keamanan siber yang relatif tinggi. Karakteristik responden penelitian adalah sebagai berikut: Jumlah responden sebanyak 115 orang, Jenis kelamin 49 laki-laki dan 66 perempuan, rentang usia: 18–23 tahun dan September–November 2025. Jumlah sampel tersebut telah memenuhi kriteria minimum analisis *Structural Equation Modeling–Partial Least Squares* (SEM-PLS), yaitu minimal 10 kali jumlah jalur terbesar menuju satu konstruk endogen.

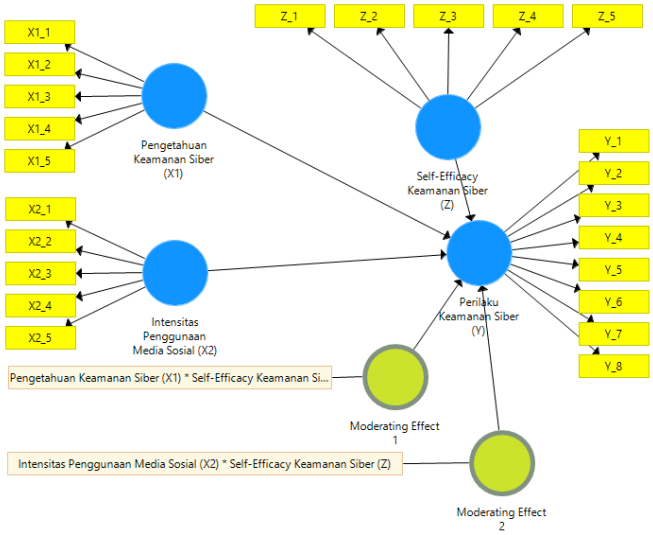
Data penelitian dikumpulkan menggunakan kuesioner tertutup yang disusun dalam bentuk skala Likert lima tingkat, mulai dari: 1 = sangat tidak setuju hingga 5 = sangat setuju. Kuesioner disebarkan secara daring kepada responden, sehingga memungkinkan pengumpulan data yang efisien dan sesuai dengan karakteristik subjek penelitian yang akrab

dengan teknologi digital. Sebelum pengisian kuesioner, responden diberikan penjelasan mengenai tujuan penelitian dan diminta untuk menyatakan persetujuan (*informed consent*) secara sukarela. Seluruh data yang dikumpulkan bersifat anonim dan hanya digunakan untuk keperluan penelitian, sehingga identitas responden tetap terjaga kerahasiaannya.

Penelitian ini melibatkan empat konstruk laten utama:

1. Pengetahuan Keamanan Siber (X1)
   Diukur menggunakan 5 indikator yang mencerminkan pemahaman responden terkait kata sandi, autentikasi dua faktor, perlindungan *malware*, risiko jaringan, dan paparan pembelajaran keamanan siber.
2. Intensitas Penggunaan Media Sosial (X2)
   Diukur menggunakan 5 indikator yang merepresentasikan durasi penggunaan, frekuensi akses, tingkat interaksi, ketergantungan informasi, serta kesulitan mengontrol penggunaan media sosial.
3. *Self-efficacy* Keamanan Siber (Z)
   Diukur menggunakan 5 indikator yang mencerminkan keyakinan individu dalam melindungi akun, mengelola pengaturan keamanan, menyelesaikan masalah keamanan, mempelajari prosedur baru, dan mengambil keputusan dalam situasi berisiko di dunia maya.
4. Perilaku Keamanan Siber (Y)
   Diukur menggunakan 8 indikator yang mencakup praktik penggunaan kata sandi aman, aktivasi autentikasi dua faktor, pengamanan perangkat, pembaruan sistem, kewaspadaan terhadap tautan mencurigakan, penghindaran Wi-Fi publik berisiko, pengendalian informasi pribadi, serta pencadangan data.

Setiap konstruk laten diukur menggunakan sejumlah indikator reflektif, di mana Pengetahuan Keamanan Siber dan Intensitas Penggunaan Media Sosial masing-masing diukur oleh lima indikator, *Self-efficacy* Keamanan Siber diukur oleh lima indikator, dan Perilaku Keamanan Siber diukur oleh delapan indikator. Efek moderasi dalam model ini direpresentasikan melalui konstruk interaksi antara X1 × Z dan X2 × Z, yang digunakan untuk menguji peran *Self-efficacy* Keamanan Siber dalam memperkuat atau memperlemah hubungan antar variabel.



Gambar 1. Model Konseptual Penelitian dengan Variabel Moderasi *Self-efficacy*

Analisis data dilakukan menggunakan metode *Structural Equation Modeling–Partial Least Squares* (SEM-PLS) dengan bantuan perangkat lunak *SmartPLS*. SEM-PLS dipilih karena mampu: 1). Mengolah konstruk laten dengan indikator majemuk, 2). Menguji model struktural yang kompleks, 3). Mengakomodasi ukuran sampel relatif moderat, dan 4). Menguji efek moderasi secara langsung dalam satu model.

Tahapan analisis data meliputi:

1. Evaluasi Model Pengukuran (*Measurement Model*)
   Evaluasi model pengukuran dilakukan untuk menilai:
   a. Validitas konvergen, melalui nilai *outer loading* ($\geqslant 0{,}70$) dan *Average Variance Extracted* (AVE $\geqslant$ 0,50) [15], [16],
   b. Reliabilitas konstruk, melalui nilai *Cronbach's Alpha*, *rho_A*, dan *Composite Reliability* ($\geqslant 0{,}70$) [17],
   c. Validitas diskriminan, melalui kriteria *Fornell–Larcker* dan *Heterotrait–Monotrait Ratio* (HTMT) (< 0,90) [18],
   d. Uji multikolinearitas, melalui nilai *Variance Inflation Factor* (VIF) (< 5) [19].
2. Evaluasi Model Struktural (*Structural Model*)
   Evaluasi model struktural dilakukan dengan menilai:
   a. Koefisien jalur (*Path Coefficients*) untuk melihat arah dan kekuatan hubungan antar konstruk [18],
   b. Koefisien determinasi (R^2 dan R^2 *Adjusted*) untuk mengukur daya jelaskan model terhadap variabel endogen[18],
   c. Uji signifikansi hipotesis, menggunakan prosedur bootstrapping dengan kriteria *t-statistic* > 1,96 pada tingkat signifikansi 5%.
   3. Pengujian Efek Moderasi

Efek moderasi *Self-efficacy* Keamanan Siber diuji menggunakan pendekatan two-stage moderation, yaitu dengan membentuk konstruk interaksi: X1 × Z → Y, X2 × Z → Y.

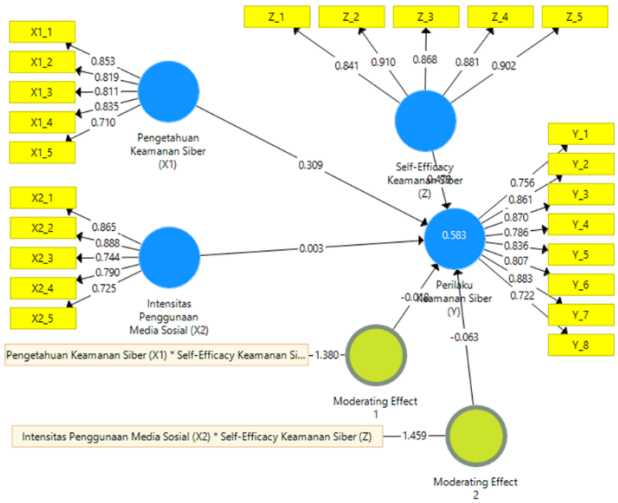
Pendekatan ini dipilih karena lebih stabil dalam menguji moderasi pada model SEM-PLS dengan konstruk reflektif. Hipotesis yang diuji dalam penelitian ini meliputi:

1. H1: Pengetahuan Keamanan Siber berpengaruh terhadap Perilaku Keamanan Siber.
2. H2: Intensitas Penggunaan Media Sosial berpengaruh terhadap Perilaku Keamanan Siber.
3. H3: *Self-efficacy* Keamanan Siber berpengaruh terhadap Perilaku Keamanan Siber.
4. H4: *Self-efficacy* Keamanan Siber memoderasi pengaruh Pengetahuan Keamanan Siber terhadap Perilaku Keamanan Siber.
5. H5: *Self-efficacy* Keamanan Siber memoderasi pengaruh Intensitas Penggunaan Media Sosial terhadap Perilaku Keamanan Siber.

III. HASIL DAN PEMBAHASAN

A. Evaluasi Model Pengukuran (*Measurement Model*)

Evaluasi model pengukuran dilakukan untuk memastikan bahwa seluruh indikator mampu merepresentasikan konstruk laten secara valid dan reliabel. Hasil analisis menunjukkan bahwa seluruh indikator pada masing-masing konstruk memiliki nilai *outer loading* $\geqslant$ 0,70, sehingga memenuhi kriteria validitas konvergen. Hal ini mengindikasikan bahwa indikator-indikator yang digunakan memiliki korelasi yang kuat dengan konstruk laten yang diukur [20].



Gambar 2. Model Struktural dan Koefisien Jalur Hasil SEM-PLS

Gambar 2 menampilkan hubungan antar variabel laten, nilai outer loading indikator, koefisien jalur antar konstruk, serta nilai koefisien determinasi (R^2) pada variabel endogen Perilaku Keamanan Siber.

Evaluasi reliabilitas dan validitas konstruk dilakukan untuk memastikan bahwa setiap variabel laten dalam model pengukuran memiliki tingkat konsistensi internal dan kemampuan representasi indikator yang memadai. Pengujian ini menggunakan kriteria *Cronbach's Alpha*, *rho_A*, *Composite Reliability*, serta *Average Variance Extracted* (AVE). Sebagai tindak lanjut dari model struktural pada Gambar 2, evaluasi reliabilitas dan validitas konstruk disajikan pada Tabel 1.

Tabel 1. Construct Reliability and Validity

Konstruk	*Cronbach's Alpha*	*rho_A*	*Composite Reliability*	*Average Variance Extracted (AVE)*
Intensitas Penggunaan Media Sosial (X2)	0.867	0.909	0.902	0.648
Moderating Effect 1	1.000	1.000	1.000	1.000
Moderating Effect 2	1.000	1.000	1.000	1.000
Pengetahuan Keamanan Siber (X1)	0.868	0.889	0.903	0.652
Perilaku Keamanan Siber (Y)	0.928	0.934	0.941	0.667
Self-efficacy Keamanan Siber (Z)	0.928	0.930	0.945	0.776

Berdasarkan Tabel 1, seluruh konstruk menunjukkan nilai *Cronbach's Alpha, rho_A,* dan *Composite Reliability* yang berada di atas ambang batas 0,70, sehingga dapat dinyatakan memiliki reliabilitas dan konsistensi internal yang baik. Selain itu, nilai AVE pada seluruh konstruk juga melebihi kriteria minimum 0,50, yang mengindikasikan terpenuhinya validitas konvergen.

Validitas diskriminan diuji untuk memastikan bahwa setiap konstruk dalam model memiliki tingkat perbedaan yang memadai satu sama lain. Pengujian validitas diskriminan dilakukan menggunakan kriteria *Fornell–Larcker*, dengan membandingkan akar kuadrat AVE pada masing-masing konstruk terhadap korelasi antar konstruk. Hasil pengujian validitas diskriminan tersebut disajikan pada Tabel 2.

Tabel 2. *Discriminant Validity (Fornell–Larcker Criterion)*

Konstruk	Intensitas Penggunaan Media Sosial (X2)	*Moderating Effect* 1	*Moderating Effect* 2	Pengetahuan Keamanan Siber (X1)	Perilaku Keamanan Siber (Y)	*Self-efficacy* Keamanan Siber (Z)
Intensitas Penggunaan Media Sosial (X2)	0.805					
Moderating Effect 1	-0.283	1.000				
Moderating Effect 2	-0.204	0.791	1.000			
Pengetahuan Keamanan Siber (X1)	0.486	-0.339	-0.268	0.807		
Perilaku Keamanan Siber (Y)	0.425	-0.335	-0.311	0.658	0.817	
Self-efficacy Keamanan Siber (Z)	0.513	-0.275	-0.243	0.656	0.712	0.881

Berdasarkan Tabel 2, nilai akar kuadrat AVE pada setiap konstruk lebih tinggi dibandingkan dengan korelasi antar konstruk lainnya, sehingga memenuhi kriteria validitas diskriminan menurut *Fornell–Larcker*. Selain itu, seluruh nilai HTMT berada di bawah ambang batas yang direkomendasikan (< 0,90), yang mengindikasikan tidak adanya masalah tumpang tindih konstruk.

Uji multikolinearitas menunjukkan bahwa nilai *Variance Inflation Factor* (VIF) seluruh indikator dan konstruk berada di bawah nilai 5. Dengan demikian, dapat disimpulkan bahwa model pengukuran dalam penelitian ini telah memenuhi seluruh kriteria validitas dan reliabilitas, sehingga layak digunakan untuk analisis model struktural.

Tabel 3. Ringkasan Nilai Variance Inflation Factor (VIF)

Model	Rentang Nilai VIF	Keterangan
Outer Model (Indikator)	1.000 – 3.099	Tidak terjadi multikolinearitas
Inner Model (Konstruk Endogen)	1.830 – 4.247	Tidak terjadi multikolinearitas

Berdasarkan Tabel 3, seluruh nilai VIF pada *outer model* dan *inner model* berada di bawah ambang batas 5, yang menunjukkan bahwa model terbebas dari permasalahan multikolinearitas. Dengan demikian, model dinyatakan layak untuk dilanjutkan pada tahap pengujian hubungan struktural.

B. Evaluasi Model Struktural (*Structural Model*)

Evaluasi model struktural dilakukan untuk menilai kemampuan model dalam menjelaskan hubungan antar variabel laten [16]. Evaluasi kekuatan prediktif model struktural dilakukan dengan mengamati nilai koefisien determinasi (R Square dan R Square Adjusted) pada variabel endogen. Nilai ini menunjukkan proporsi variansi konstruk endogen yang dapat dijelaskan oleh konstruk eksogen dalam model. Hasil pengujian tersebut disajikan pada Tabel X.

Tabel 4. Nilai R Square dan R Square Adjusted

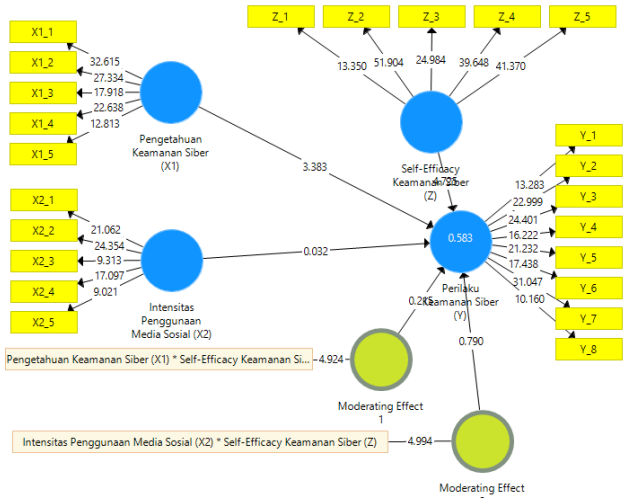
Variabel Endogen	*R Square* (R^2)	*R Square Adjusted*
Perilaku Keamanan Siber (Y)	0.583	0.564

Berdasarkan Tabel 4, nilai *R Square* sebesar 0.583 menunjukkan bahwa sebesar 58,3% variansi Perilaku

Keamanan Siber dapat dijelaskan oleh variabel-variabel prediktor dalam model, sedangkan sisanya dipengaruhi oleh faktor lain di luar model. Nilai *R Square Adjusted* sebesar 0.564 mengindikasikan bahwa kemampuan penjelasan model tetap berada pada tingkat moderat setelah mempertimbangkan kompleksitas model, sehingga model struktural memiliki daya jelaskan yang memadai.

C. Pengujian Hipotesis dan Hasil *Bootstrapping*

Pengujian hipotesis dilakukan menggunakan prosedur *bootstrapping* untuk menilai signifikansi koefisien jalur antar konstruk. Hasil analisis koefisien jalur menunjukkan beberapa temuan penting.



Gambar 3. Model Struktural dengan Nilai *t-Statistics* Hasil *Bootstrapping*

Gambar 3 menampilkan nilai *t-statistics* pada setiap jalur struktural, indikator, serta konstruk interaksi moderasi yang digunakan untuk menguji hipotesis penelitian.

Pengujian hubungan struktural dilakukan untuk menguji pengaruh langsung variabel eksogen terhadap variabel endogen dalam model. Evaluasi dilakukan menggunakan analisis koefisien jalur (*Path Coefficients*) melalui prosedur bootstrapping, dengan kriteria signifikansi berdasarkan nilai *t-statistics* dan *p-values*. Sebagai tindak lanjut dari model struktural pada Gambar 3, Koefisien Jalur disajikan pada Tabel 5.

Tabel 5. Hasil Uji Koefisien Jalur (*Path Coefficients*)

Hubungan Antar Variabel	*Original Sample (O)*	*Sample Mean (M)*	*Standard Deviation*	*T-Statistics*	*P-values*
Intensitas Penggunaan Media Sosial (X2) → Perilaku Keamanan Siber (Y)	0.003	0.005	0.084	0.032	0.975
Moderating Effect 1 → Perilaku Keamanan Siber (Y)	-0.018	-0.016	0.083	0.215	0.830
Moderating Effect 2 → Perilaku Keamanan Siber (Y)	-0.063	-0.057	0.080	0.790	0.430
Pengetahuan Keamanan Siber (X1) → Perilaku Keamanan Siber (Y)	0.309	0.315	0.091	3.383	0.001
Self-efficacy Keamanan Siber (Z) → Perilaku Keamanan Siber (Y)	0.479	0.476	0.101	4.725	0.000

Pengujian hipotesis dalam penelitian ini dilakukan dengan menganalisis koefisien jalur (*Path Coefficients*) menggunakan prosedur *bootstrapping* pada SEM-PLS. Evaluasi signifikansi hubungan antar konstruk didasarkan pada nilai *t-statistic* > 1,96 dan *p-value* < 0,05 pada tingkat signifikansi 5%.

Hasil analisis menunjukkan bahwa Pengetahuan Keamanan Siber (X1) memiliki pengaruh positif dan signifikan terhadap Perilaku Keamanan Siber (Y), dengan nilai koefisien jalur sebesar 0,309, nilai *t-statistic* sebesar 3,383, dan *p-value* sebesar 0,001. Temuan ini mengindikasikan bahwa peningkatan pengetahuan keamanan siber secara nyata berkontribusi terhadap peningkatan perilaku keamanan siber pengguna.

Sebaliknya, Intensitas Penggunaan Media Sosial (X2) tidak menunjukkan pengaruh yang signifikan terhadap Perilaku Keamanan Siber (Y). Hal ini ditunjukkan oleh nilai koefisien jalur sebesar 0,003, nilai *t-statistic* sebesar 0,032, dan *p-value* sebesar 0,975. Temuan ini mengindikasikan bahwa intensitas penggunaan media sosial, secara langsung, tidak cukup kuat untuk memengaruhi perilaku keamanan siber.

Selanjutnya, hasil pengujian menunjukkan bahwa *Self-efficacy* Keamanan Siber (Z) berpengaruh positif dan signifikan terhadap Perilaku Keamanan Siber (Y), dengan nilai koefisien jalur sebesar 0,479, nilai *t-statistic* sebesar 4,725, dan *p-value* sebesar 0,000. Hal ini menegaskan bahwa keyakinan individu terhadap kemampuannya dalam mengelola risiko siber merupakan determinan penting dalam pembentukan perilaku keamanan siber.

Terkait dengan pengujian efek moderasi, baik Moderating Effect 1 (X1 × Z → Y) maupun Moderating Effect 2 (X2 × Z → Y) tidak menunjukkan pengaruh yang signifikan terhadap Perilaku Keamanan Siber (Y). Moderating Effect 1 memiliki nilai koefisien jalur sebesar –0,018 dengan *t-statistic* sebesar 0,215 dan *p-value* sebesar 0,830, sedangkan Moderating Effect 2 memiliki nilai koefisien jalur sebesar –0,063 dengan *t-statistic* sebesar 0,790 dan *p-value* sebesar 0,430. Temuan ini mengindikasikan bahwa *Self-efficacy* keamanan siber tidak berperan sebagai variabel moderator dalam hubungan antara pengetahuan keamanan siber maupun intensitas penggunaan media sosial terhadap perilaku keamanan siber.

E. Pembahasan

Pembahasan hasil pengujian hipotesis difokuskan pada evaluasi hubungan kausal antar variabel laten dalam model struktural. Pengujian dilakukan menggunakan analisis koefisien jalur (*Path Coefficients*) melalui prosedur bootstrapping untuk menilai arah, kekuatan, dan signifikansi pengaruh antar konstruk. Keputusan penerimaan atau penolakan hipotesis didasarkan pada nilai *t-statistics* dan *p-values*. Ringkasan hasil pengujian hubungan struktural tersebut disajikan pada Tabel 6.

Tabel 6. Keputusan hipotesis

Jalur Hipotesis	Koefisien (O)	*T-Statistics*	*P-Values*	Keputusan
Intensitas Penggunaan Media Sosial (X2) → Perilaku Keamanan Siber (Y)	0.003	0.032	0.975	Ditolak
Moderating Effect 1 → Perilaku Keamanan Siber (Y)	-0.018	0.215	0.830	Ditolak
Moderating Effect 2 → Perilaku Keamanan Siber (Y)	-0.063	0.790	0.430	Ditolak
Pengetahuan Keamanan Siber (X1) → Perilaku Keamanan Siber (Y)	0.309	3.383	0.001	Diterima
Self-efficacy Keamanan Siber (Z) → Perilaku Keamanan Siber (Y)	0.479	4.725	0.000	Diterima

Hasil penelitian ini menunjukkan bahwa perilaku keamanan siber pada pengguna media sosial lebih ditentukan oleh faktor kognitif dan psikologis internal dibandingkan oleh tingkat penggunaan media sosial itu sendiri. Pengetahuan keamanan siber berperan sebagai fondasi kognitif yang memungkinkan individu mengenali risiko dan memahami langkah-langkah perlindungan yang tepat. Temuan menunjukkan bahwa efektivitas pengetahuan keamanan siber dalam mendorong perilaku protektif sangat bergantung pada tingkat *Self-efficacy* individu [21].

Peran dominan *Self-efficacy* dalam penelitian ini menegaskan bahwa upaya peningkatan perilaku keamanan siber tidak cukup hanya dengan memberikan informasi atau pelatihan teknis. Penguatan keyakinan individu terhadap kemampuannya untuk mengelola risiko digital menjadi faktor kunci agar perilaku protektif dapat diterapkan secara konsisten. Temuan ini sejalan dengan pandangan SCT yang menekankan bahwa perilaku merupakan hasil interaksi antara faktor personal, lingkungan, dan tindakan individu [22], [23].

Tidak signifikannya pengaruh intensitas penggunaan media sosial menunjukkan bahwa tingginya keterlibatan digital tidak secara otomatis mendorong perilaku aman atau tidak aman. Hal ini mengimplikasikan bahwa risiko keamanan siber pada pengguna media sosial lebih bersifat *behavior-driven* daripada *exposure-driven* [24], [25]. Dengan demikian, intervensi keamanan siber yang efektif perlu difokuskan pada pengembangan kompetensi dan kepercayaan diri pengguna, bukan sekadar pembatasan penggunaan media sosial.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa:

a. Pengetahuan keamanan siber berpengaruh signifikan terhadap perilaku keamanan siber.
b. Intensitas penggunaan media sosial tidak berpengaruh signifikan terhadap perilaku keamanan siber.
c. *Self-efficacy* keamanan siber berpengaruh signifikan dan menjadi prediktor terkuat perilaku keamanan siber.
d. *Self-efficacy* tidak berperan sebagai variabel moderasi, melainkan sebagai faktor langsung.

IV. KESIMPULAN

Penelitian ini menganalisis determinan perilaku keamanan siber pada pengguna media sosial dengan mengintegrasikan pengetahuan keamanan siber, intensitas penggunaan media sosial, dan *Self-efficacy* keamanan siber dalam satu model empiris yang berlandaskan *Protection Motivation Theory* (PMT) dan *Social Cognitive Theory* (SCT). Hasil analisis menggunakan pendekatan SEM-PLS menunjukkan bahwa pengetahuan keamanan siber dan *Self-efficacy* keamanan siber berpengaruh positif dan signifikan terhadap perilaku keamanan siber, sedangkan intensitas penggunaan media sosial tidak menunjukkan pengaruh yang signifikan.

Self-efficacy keamanan siber muncul sebagai prediktor paling dominan dalam membentuk perilaku keamanan siber. Namun, perannya sebagai variabel moderasi tidak terbukti, sehingga *Self-efficacy* lebih tepat dipahami sebagai faktor internal langsung yang memengaruhi perilaku keamanan siber, bukan sebagai variabel yang memperkuat atau memperlemah hubungan antar variabel lainnya.

Temuan ini mengindikasikan bahwa perilaku keamanan siber pada pengguna media sosial lebih dipengaruhi oleh faktor kognitif dan psikologis internal dibandingkan oleh tingkat penggunaan media sosial itu sendiri. Secara praktis, upaya peningkatan keamanan siber, khususnya di lingkungan pendidikan tinggi, sebaiknya difokuskan pada penguatan pengetahuan keamanan siber dan peningkatan *Self-efficacy* melalui pembelajaran berbasis praktik dan simulasi ancaman, bukan semata-mata pada pembatasan penggunaan media sosial.

Penelitian ini memiliki keterbatasan pada lingkup sampel yang berasal dari satu institusi, sehingga generalisasi hasil penelitian masih terbatas. Penelitian selanjutnya disarankan untuk melibatkan subjek yang lebih beragam serta mempertimbangkan variabel lain, seperti persepsi risiko, norma sosial, atau pengalaman belajar, guna memperoleh pemahaman yang lebih komprehensif mengenai perilaku keamanan siber.

DAFTAR PUSTAKA

[1] L. M. Ganiem, R. Setiawati, S. Suardi, N. Nurhayai, and R. Ramdhani, "Society in the Digital Era: Adaptation, Change, and Response to Communication Technology," *J. Int. Dakwah Commun.*, vol. 4, no. 1, pp. 123–135, June 2024, doi: 10.55849/jidc.v4i1.639.

[2] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of Social Media," *Bus. Horiz.*, vol. 53, no. 1, pp. 59–68, Jan. 2010, doi: 10.1016/j.bushor.2009.09.003.

[3] N. B. Ellison, C. Steinfield, and C. Lampe, "The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites," *J. Comput.-Mediat. Commun.*, vol. 12, no. 4, pp. 1143–1168, July 2007, doi: 10.1111/j.1083-6101.2007.00367.x.

[4] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *J. Comput.-Mediat. Commun.*, vol. 13, no. 1, pp. 210–230, Oct. 2007, doi: 10.1111/j.1083-6101.2007.00393.x.

[5] E. Mouncey and S. Ciobotaru, "Phishing scams on social media: An evaluation of cyber awareness education on

impact and effectiveness," *J. Econ. Criminol.*, vol. 7, p. 100125, Mar. 2025, doi: 10.1016/j.jeconc.2025.100125.
[6] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Front. Comput. Sci.*, vol. 3, p. 563060, Mar. 2021, doi: 10.3389/fcomp.2021.563060.
[7] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Jan. 2022, doi: 10.1080/08874417.2020.1712269.
[8] H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Comput. Secur.*, vol. 28, no. 8, pp. 816–826, Nov. 2009, doi: 10.1016/j.cose.2009.05.008.
[9] U. Kiran, N. F. Khan, H. Murtaza, A. Farooq, and H. Pirkkalainen, "Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory," *Comput. Secur.*, vol. 149, p. 104204, Feb. 2025, doi: 10.1016/j.cose.2024.104204.
[10] N. Borgert, L. Jansen, I. Böse, J. Friedauer, M. A. Sasse, and M. Elson, "Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, Honolulu HI USA: ACM, May 2024, pp. 1–32. doi: 10.1145/3613904.3642432.
[11] S. Prabhu and P. Pathak, "Impact of Social Media User Anxieties, Privacy and Security Issues, and Self-Regulation on User Behavior," *J. Scientometr. Res.*, vol. 14, no. 2, pp. 510–524, Sept. 2025, doi: 10.5530/jscires.20251200.
[12] S. F. Nagari and S. Raharja, "Cyber Security Awareness, Knowledge and Behavior of Digital Banking Users in Salatiga," *Asia Pac. Fraud J.*, vol. 10, no. 1, pp. 15–29, July 2025, doi: 10.21532/apfjournal.v10i1.398.
[13] William Vortia, "Modelling cybersecurity awareness, perceived threats and secure online behavioral intentions among Ghanaian university students: A PLS-SEM Approach," *Magna Sci. Adv. Res. Rev.*, vol. 14, no. 2, pp. 096–111, Aug. 2025, doi: 10.30574/msarr.2025.14.2.0094.
[14] M. Gustara, E. R. Cahyadi, and B. Sartono, "ANALYSIS OF CYBERSECURITY AWARENESS AND BEHAVIOR AMONG STUDENTS OF IPB UNIVERSITY: AN INTEGRATION OF PROTECTION MOTIVATION THEORY AND THEORY OF PLANNED BEHAVIOR," vol. 8, no. 3, 2025.
[15] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *J. Mark. Res.*, vol. 18, no. 1, pp. 39–50, Feb. 1981, doi: 10.1177/002224378101800104.
[16] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *Eur. Bus. Rev.*, vol. 31, no. 1, pp. 2–24, Jan. 2019, doi: 10.1108/EBR-11-2018-0203.
[17] L. M. Pereira, V. Sanchez Rodrigues, and F. G. M. Freires, "Use of Partial Least Squares Structural Equation Modeling (PLS-SEM) to Improve Plastic Waste Management," *Appl. Sci.*, vol. 14, no. 2, p. 628, Jan. 2024, doi: 10.3390/app14020628.
[18] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*. in Classroom Companion: Business. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-80519-7.
[19] R. M. O'brien, "A Caution Regarding Rules of Thumb for Variance Inflation Factors," *Qual. Quant.*, vol. 41, no. 5, pp. 673–690, Sept. 2007, doi: 10.1007/s11135-006-9018-6.
[20] A. Sukhov, M. Friman, and L. E. Olsson, "Unlocking potential: An integrated approach using PLS-SEM, NCA, and fsQCA for informed decision making," *J. Retail. Consum. Serv.*, vol. 74, p. 103424, Sept. 2023, doi: 10.1016/j.jretconser.2023.103424.
[21] R. Shillair, S. R. Cotten, H.-Y. S. Tsai, S. Alhabash, R. LaRose, and N. J. Rifon, "Online safety begins with you and me: Convincing Internet users to protect themselves," *Comput. Hum. Behav.*, vol. 48, pp. 199–207, July 2015, doi: 10.1016/j.chb.2015.01.046.
[22] S. Zhai, J. Hash, T. M. Ward, W. Yuwen, and J. Sonney, "Analysis, evaluation, and reformulation of social cognitive theory: Toward parent-child shared management in sleep health," *J. Pediatr. Nurs.*, vol. 73, pp. e65–e74, Nov. 2023, doi: 10.1016/j.pedn.2023.07.011.
[23] R. Wood and A. Bandura, "Social Cognitive Theory of Organizational Management," *Acad. Manage. Rev.*, vol. 14, no. 3, p. 361, July 1989, doi: 10.2307/258173.
[24] E. D. Frauenstein and S. Flowerday, "Susceptibility to phishing on social network sites: A personality information processing model," *Comput. Secur.*, vol. 94, p. 101862, July 2020, doi: 10.1016/j.cose.2020.101862.
[25] Y. Hong and S. Furnell, "Understanding cybersecurity behavioral habits: Insights from situational support," *J. Inf. Secur. Appl.*, vol. 57, p. 102710, Mar. 2021, doi: 10.1016/j.jisa.2020.102710.