TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

Analisis Perilaku Kesadaran Privasi Data Pengguna Sistem Informasi Akademik dengan Pendekatan Technology Threat Avoidance Theory

Yusrizal Hamdi*, Catur Eri Gunawan, Imamulhakim Syahid Putra

Fakultas Sains dan Teknologi, Prodi Sistem Informasi, Universitas Islam Negeri Raden Fatah Palembang, Palembang, Indonesia
Email: 1,*yusrizalhamdi@gmail.com, 2caturerig@radenfatah.ac.id, 3imamulhakim_uin@radenfatah.ac.id
Email Penulis Korespondensi: yusrizalhamdi@gmail.com

Abstrak−Implementasi Sistem Informasi Akademik (SIMAK) memunculkan kekhawatiran terkait aspek keamanan data, khususnya yang menyangkut privasi data pribadi, nilai akademik, serta data Kartu Rencana Studi (KRS). Ancaman terhadap privasi data pengguna kerap kali bersumber dari aktor internal, yang berpotensi mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Penelitian ini bertujuan untuk mengeksplorasi berbagai faktor yang memengaruhi perilaku kesadaran pengguna SIMAK dalam menghadapi ancaman terhadap privasi data, melalui pendekatan *Technology Threat Avoidance Theory* (*TTAT*). Pendekatan penelitian yang digunakan bersifat kuantitatif, dengan pengumpulan data melalui kuesioner yang disebarkan kepada 393 responden, terdiri atas mahasiswa dan dosen pengguna aktif SIMAK. Data yang terkumpul dianalisis menggunakan metode *Covariance-Based Structural Equation Modelling* (*CB-SEM*) dengan perangkat lunak SmartPLS 4. Hasil penelitian mengungkapkan bahwa persepsi terhadap kerentanan dan keparahan, beserta interaksinya, memiliki pengaruh positif terhadap persepsi ancaman. Persepsi ancaman ini terbukti secara signifikan meningkatkan motivasi untuk menghindari risiko. Namun, interaksi antara persepsi ancaman dan efektivitas tindakan pengamanan justru menunjukkan dampak negatif. Di sisi lain, efikasi diri berperan positif dalam mendorong motivasi penghindaran, yang pada akhirnya turut membentuk perilaku kesadaran dalam melindungi privasi data. Temuan ini menyoroti pentingnya peningkatan kesadaran serta kemampuan individu dalam menjaga keamanan informasi pada sistem informasi akademik.

Kata Kunci: Analisis**;** Perilaku Kesadaran; Privasi Data; SIMAK; *TTAT*

Abstract−The implementation of the *Sistem Informasi Akademik* (*SIMAK*) has raised concerns regarding data security, particularly the privacy of personal data, academic grades, and *Kartu Rencana Studi* (*KRS*) information. Threats to user data privacy often originate from internal actors, posing risks to the confidentiality, integrity, and availability of information. This study aims to explore the factors influencing SIMAK users' privacy awareness behavior in response to such threats, using the Technology Threat Avoidance Theory (TTAT) as a theoretical framework. A quantitative research approach was employed, with data collected through questionnaires distributed to 393 respondents, comprising active SIMAK users from both student and faculty groups. The collected data were analyzed using the Covariance-Based Structural Equation Modeling (CB-SEM) method with the SmartPLS 4 software. The results reveal that perceptions of vulnerability and severity, as well as their interaction, positively influence threat perception. This perceived threat significantly enhances the motivation to avoid risks. However, the interaction between threat perception and safeguard effectiveness shows a negative impact. On the other hand, self-efficacy positively contributes to avoidance motivation, which in turn influences users' awareness behavior in protecting data privacy. These findings emphasize the importance of enhancing individual awareness and capability in maintaining information security within academic information systems.

Keywords: Analysis; Awareness Behavior; Data Privacy; *SIMAK*; TTAT

1. PENDAHULUAN

Kemajuan pesat dalam teknologi informasi saat ini mendorong setiap organisasi, termasuk lembaga pendidikan tinggi, untuk mengintegrasikan sistem digital dalam proses bisnis mereka. Penerapan sistem informasi akademik menjadi langkah strategis guna meningkatkan efisiensi dan efektivitas pelayanan akademik. Namun demikian, kompleksitas sistem informasi yang diterapkan di lingkungan perguruan tinggi memunculkan tantangan baru terkait dengan keamanan data dan perlindungan privasi pengguna. Data akademik seperti data pribadi, nilai, dan Kartu Rencana Studi (KRS) merupakan informasi sensitif yang perlu dijaga kerahasiaannya untuk mencegah penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab.

Universitas Islam Negeri (UIN) Raden Fatah Palembang adalah salah satu lembaga pendidikan tinggi yang sedang aktif mengembangkan berbagai sistem informasi untuk mendukung proses akademik. Salah satu sistem yang menjadi inti dalam pengelolaan data akademik di lingkungan kampus ini adalah Sistem Informasi Akademik (SIMAK). Sistem ini digunakan secara aktif oleh mahasiswa dan dosen untuk mengakses dan mengelola data akademik seperti biodata, nilai, serta kartu rencana studi (KRS) (Ramayani *et al*., 2022). Namun, berdasarkan hasil observasi dan wawancara pada pra-penelitian yang dilakukan, ditemukan adanya sejumlah permasalahan terkait ancaman terhadap privasi data pengguna SIMAK. Permasalahan tersebut di antaranya meliputi pemberian akses akun SIMAK kepada pihak lain, penggantian kata sandi secara tidak sah, hingga terhapusnya data KRS oleh pihak yang bukan pemilik akun. Ancaman ini umumnya tidak hanya berasal dari serangan eksternal, melainkan juga dari aktor internal yang menjadi bagian dari sistem itu sendiri, sehingga termasuk dalam kategori *personal security threat* (Razzaq *et al*., 2022).

Penggunaan sistem informasi yang tidak diiringi dengan kesadaran terhadap ancaman privasi data dapat meningkatkan risiko kebocoran dan penyalahgunaan informasi. Karena itu, diperlukan pemahaman yang lebih mendalam mengenai perilaku pengguna dalam menghadapi ancaman privasi tersebut. Salah satu pendekatan yang relevan untuk menganalisis perilaku ini adalah *Technology Threat Avoidance Theory* (*TTAT*) yang dikembangkan oleh (Liang & Xue, 2010). TTAT mengkaji bagaimana pengguna sistem informasi merespons ancaman terhadap keamanan data melalui beberapa konstruk penting, seperti persepsi kerntanan *(perceived susceptibility)*, persepsi keparahan *(perceived severity)*, persepsi ancaman *(perceived threat)*, efektivitas pengamanan *(safeguard effectiveness)*, biaya

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

pengamanan *(safeguard cost)*, efikasi diri *(self-efficacy)*, motivasi penghindaran *(avoidance motivation)*, dan perilaku penghindaran *(avoidance behaviour)*. Teori ini menekankan bahwa persepsi pengguna terhadap ancaman dan efektivitas tindakan pengamanan akan memengaruhi motivasi dan perilaku mereka dalam menghindari risiko.

Beberapa penelitian terdahulu telah mengadopsi pendekatan TTAT untuk menganalisis perilaku pengguna terhadap ancaman privasi data. Penelitian terdahulu menemukan bahwa *perceived susceptibility* dan *perceived severity* berpengaruh positif terhadap *perceived threat* (Carpenter *et al*., 2019; Mark *et al*., 2021; Sylvester, 2022). Penelitian lain, menunjukkan bahwa *perceived threat* tidak selalu berdampak langsung pada *avoidance motivation* (Djatsa, 2020), menunjukkan bahwa hubungan antar variabel dalam TTAT tidak selalu konsisten. Penelitian lain juga mendukung pengaruh positif dari *safeguard effectiveness* terhadap motivasi penghindaran (Butler, 2020; Saidi & Prayudi, 2021). Namun, *safeguard cost* tidak selalu memiliki pengaruh terhadap motivasi penghindaran (Arachchilage & Love, 2014), menandakan adanya ketidakkonsistenan yang perlu dikaji lebih lanjut. Selain itu, efikasi diri ditemukan secara konsisten memiliki pengaruh positif terhadap motivasi penghindaran dalam beberapa studi seperti yang dilakukan (Gillam & Foster, 2020; Tang *et al*., 2021).

Dari hasil studi terdahulu tersebut, terlihat adanya perbedaan hasil atau *research gap* dalam pengujian hubungan antar variabel TTAT, terutama pada hubungan antara *perceived threat* dengan *avoidance motivation*, dan *safeguard cost* terhadap *avoidance motivation*. Gap ini menjadi dasar penting untuk dilakukan replikasi studi pada konteks yang berbeda, khususnya pada pengguna SIMAK di Indonesia, mengingat konteks pengguna sistem informasi di perguruan tinggi di Indonesia memiliki karakteristik unik yang belum banyak dieksplorasi. Selain itu, sejauh penelusuran penulis, belum terdapat studi yang secara khusus meneliti perilaku kesadaran pengguna dalam menghindari ancaman terhadap privasi data pada sistem informasi akademik SIMAK dengan pendekatan TTAT, terutama di lingkungan UIN Raden Fatah Palembang.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengeksplorasi berbagai faktor yang memengaruhi perilaku kesadaran pengguna SIMAK dalam menghadapi ancaman terhadap privasi data melalui pendekatan *TTAT*. Penelitian ini akan melibatkan responden dari kalangan mahasiswa dan dosen aktif pengguna SIMAK, dan menggunakan pendekatan kuantitatif dengan metode analisis *Covariance-Based Structural Equation Modelling* (*CB-SEM*). Temuan dari penelitian ini tidak hanya memberikan kontribusi akademik dalam memperkaya literatur tentang TTAT dan perilaku keamanan informasi, tetapi juga memberikan masukan praktis bagi pengembang sistem dan pengelola kebijakan di lingkungan perguruan tinggi untuk merancang strategi peningkatan kesadaran keamanan data yang lebih efektif, khususnya dalam konteks penggunaan SIMAK. Dengan begitu, implementasi sistem informasi akademik dapat berjalan dengan lebih aman, efisien, dan mendukung terciptanya tata kelola informasi yang lebih baik di lingkungan kampus.

2. METODOLOGI PENELITIAN

2.1 Kajian Teoritis Penelitian

Perilaku kesadaran berkaitan dengan bagaimana individu mengidentifikasi, merespons, dan bertindak terhadap potensi ancaman terhadap keamanan dan privasi data mereka. Hansch & Benenson (2014) membahas bahwa kesadaran ini dapat dilihat dari tiga perspektif: kesadaran sebagai persepsi, pengamanan, dan perilaku. Ketiga aspek ini penting untuk memahami bagaimana pengguna teknologi, seperti aplikasi SIMAK, mempertimbangkan potensi risiko dan ancaman yang dapat mempengaruhi privasi data mereka.

Privasi data menjadi isu yang semakin penting di era digital ini. Privasi data mengacu pada perlindungan informasi pribadi dari akses yang tidak sah atau penyalahgunaan oleh pihak ketiga (Shokri *et al*., 2017). Konsep ini terkait erat dengan keamanan data, namun keduanya tidak identik. Privasi lebih menekankan pada pengendalian akses terhadap informasi pribadi, sedangkan keamanan berfokus pada langkah-langkah teknis untuk melindungi data dari ancaman luar. Penelitian ini berfokus pada bagaimana kesadaran terhadap privasi data memengaruhi perilaku pengguna dalam melindungi informasi pribadi mereka, khususnya dalam penggunaan sistem informasi akademik seperti SIMAK.

SIMAK adalah sistem berbasis website yang dirancang untuk memenuhi kebutuhan layanan akademik bagi civitas akademika (Dzihni *et al*., 2019). SIMAK memungkinkan penggunanya untuk mengakses berbagai informasi akademik secara online kapan saja dan di mana saja. Aplikasi ini memiliki fungsi penting dalam mendukung proses pendidikan, namun juga berpotensi menimbulkan risiko terkait dengan privasi dan keamanan data pengguna (Restama & Efni, 2014). Oleh karena itu, penting untuk menganalisis bagaimana kesadaran privasi data berpengaruh terhadap perilaku pengguna SIMAK oleh penggunanya, serta bagaimana fitur pengamanan diterapkan dalam platform ini.

Salah satu pendekatan yang relevan untuk menganalisis perilaku ini adalah *Technology Threat Avoidance Theory* (*TTAT*) yang dikembangkan oleh Liang & Xue (2010). TTAT mengkaji bagaimana pengguna sistem informasi merespons ancaman terhadap keamanan data melalui beberapa konstruk penting, seperti persepsi kerntanan *(perceived susceptibility)*, persepsi keparahan *(perceived severity)*, persepsi ancaman *(perceived threat)*, efektivitas pengamanan *(safeguard effectiveness)*, biaya pengamanan *(safeguard cost)*, efikasi diri *(self-efficacy)*, motivasi penghindaran *(avoidance motivation)*, dan perilaku penghindaran *(avoidance behaviour)*. Teori ini menekankan bahwa persepsi pengguna terhadap ancaman dan efektivitas tindakan pengamanan akan memengaruhi motivasi dan perilaku mereka dalam menghindari risiko.

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

2.2 Kerangka Dasar Penelitian

2.2.1 Jenis Penelitian

Penelitian ini mengaplikasikan metode kuantitatif karena fokus utamanya pada populasi atau sampel tertentu, data yang dikumpulkan berupa angka untuk menjelaskan dan menguji hipotesis (Sugiyono, 2019). Penelitian menggunakan metode kuantitatif karena telah dirumuskan permasalahan yang ada yang menggunakan teori *TTAT* untuk menyelesaikan permasalahan penelitian.

2.2.2 Jumlah Responden

Objek penelitian adalah Sistem Informasi Akademik (SIMAK) UIN Raden Fatah Palembang, dengan populasi pengguna berjumlah 22.457, terdiri dari 21.861 mahasiswa dan 596 dosen aktif. Sampel diambil menggunakan metode snowball sampling yang efisien secara biaya dan waktu (Machali, 2021). Jumlah sampel dihitung dengan rumus slovin dengan tingkat kesalahan 5%. Perhitungan sampel ditunjukkan pada rumus (1).

$$n = \frac{N}{1+\mathrm{N}(e)^2} \tag{1}$$

Perhitungan jumlah sampel dalam penelitian ini menggunakan rumus (1), di mana n merupakan jumlah sampel yang diperlukan, N adalah jumlah populasi, dan e merupakan tingkat kesalahan pengambilan sampel (*sampling error*) yang biasanya ditetapkan sebesar 5% atau 0,05. Rumus ini digunakan untuk menentukan jumlah sampel yang representatif dari keseluruhan populasi dengan mempertimbangkan batas toleransi kesalahan, sehingga hasil penelitian dapat digeneralisasikan dengan tingkat kepercayaan yang tinggi.

$$n = \frac{22.457}{1+(0.5)^2} = 393$$

Perhitungan sampel dengan rumus slovin mendapatkan sampel sebanyak 393 responden. Selanjutnya, sampel tersebut dibagi secara proporsional menggunakan metode *proportional random sampling* agar representatif (Machali, 2021). Perhitungan sampel dengan metode *proportional random sampling* ditunjukkan pada rumus (2).

$$ni = \frac{Ni}{N}n \tag{2}$$

Perhitungan sampel dengan metode *proportional random sampling* dilakukan menggunakan rumus (2), dimana n_i merupakan ukuran sampel untuk strata ke-*i*, N_i adalah jumlah populasi pada strata ke-*i*, *N* merupakan total populasi, dan *n* adalah jumlah total sampel yang telah diperoleh dari perhitungan menggunakan rumus Slovin. Rumus ini bertujuan untuk membagi jumlah sampel secara proporsional berdasarkan ukuran masing-masing strata dalam populasi, sehingga distribusi sampel mencerminkan proporsi sebenarnya dari setiap kelompok dalam populasi.

$$\text{n mahasiswa} = \frac{21.861}{22.457}393 = 383$$

$$\text{n dosen} = \frac{596}{22.457}393 = 10$$

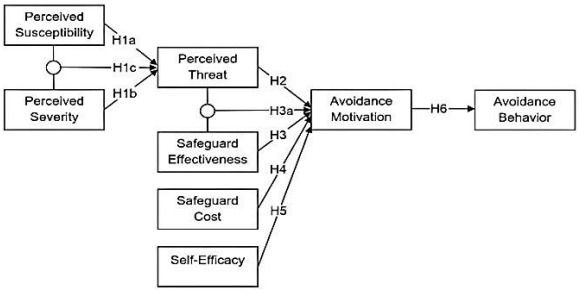
Perhitungan sampel dengan rumus proportional random sampling membagi sampel secara proporsional menjadi 383 mahasiswa dan 10 dosen sebagai responden penelitian.

2.2.3 Lokasi Penelitian

Penelitian dilakukan di Kampus A Universitas Islam Negeri Raden Fatah Palembang yang beralamatkan di Jl.Prof.K.H.Zainal Abidin Fikri KM.3,5 Palembang dan Kampus B yang beralamatkan di Jl. Pangeran Ratu (Jakabaring), Kelurahan 5 Ulu, Kecamatan Seberang Ulu I, Kota Palembang.

2.2.4 Hipotesis dan Variabel

Berdasarkan teori *TTAT* terdapat 8 variabel yang terdiri dari 5 variabel independen dan 3 variabel dependen. Sehingga telah dirumuskan hipotesis penelitian sebanyak 9 hipotesis. Hipotesis penelitian dan variabel ditunjukkan pada gambar 1.



Gambar 1. Hipotesis Penelitian

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

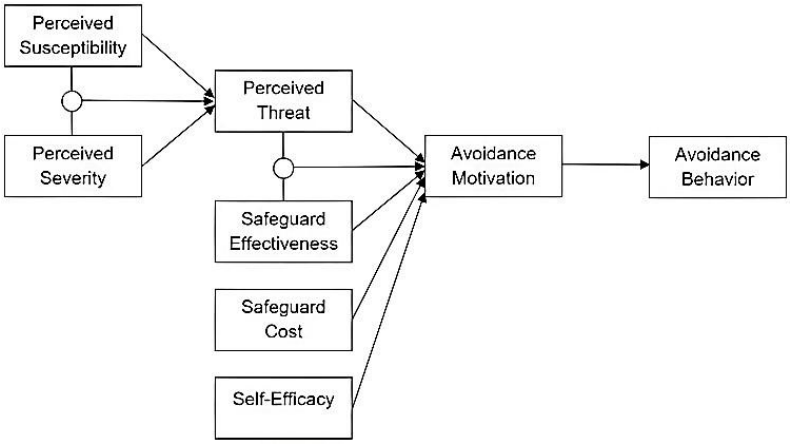
1. Hipotesis 1a:
   Ho: Persepsi kerentanan terhadap ancaman keamanan pribadi tidak memengaruhi persepsi ancaman.
   Ha: Persepsi kerentanan terhadap ancaman keamanan pribadi memengaruhi persepsi ancaman.
2. Hipotesis 1b:
   Ho: Persepsi keparahan terhadap ancaman keamanan pribadi tidak memengaruhi persepsi ancaman.
   Ha: Persepsi keparahan terhadap ancaman keamanan pribadi memengaruhi persepsi ancaman.
3. Hipotesis 1c:
   Ho: Persepsi kerentanan dan persepsi keparahan tidak memiliki efek interaksi terhadap persepsi ancaman.
   Ha: Persepsi kerentanan dan persepsi keparahan memiliki efek interaksi terhadap persepsi ancaman.
4. Hipotesis 2:
   Ho: Persepsi ancaman tidak memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
   Ha: Persepsi ancaman memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
5. Hipotesis 3:
   Ho: Efektivitas pengamanan tidak memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
   Ha: Efektivitas pengamanan memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
6. Hipotesis 3a:
   Ho: Persepsi ancaman dan efektivitas pengamanan tidak memiliki efek interaksi terhadap motivasi untuk menghindari ancaman keamanan pribadi.
   Ha: Persepsi ancaman dan efektivitas pengamanan memiliki efek interaksi terhadap motivasi untuk menghindari ancaman keamanan pribadi.
7. Hipotesis 4:
   Ho: Biaya pengamanan tidak memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
   Ha: Biaya pengamanan memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
8. Hipotesis 5:
   Ho: Efikasi diri tidak memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
   Ha: Efikasi diri memengaruhi motivasi untuk menghindari ancaman keamanan pribadi.
9. Hipotesis 6:
   Ho: Motivasi penghindaran tidak memengaruhi perilaku kesadaran untuk menghindari ancaman keamanan pribadi dalam menggunakan pengamanan.
   Ha: Motivasi penghindaran memengaruhi perilaku kesadaran untuk menghindari ancaman keamanan pribadi dalam menggunakan pengamanan.

2.2.5 Teknik Analisis

Analisis data menggunakan *Covariance Based Structural Equation Modelling* (*CB-SEM*). Analisis *CB-SEM* menurut Waluyo & Rachman (2020) umumnya terbagi menjadi dua sub-model, yakni model pengukuran yang sering disebut outer model dan model struktural yang sering disebut sebagai inner model. Outer model digunakan untuk menguji reliabilitas, validitas konvergen, validitas diskriminan, dan Goodness of Fit. Inner model digunakan dalam hal pengujian hipotesis. Pada outer model variabel harus saling terkait (*covariance*), sedangkan pada uji inner model, hubungan antara variabel sesuai dengan hipotesis atau teori yang ada (Siregar *et al*., 2021).

2.2.6 Kerangka Pemikiran

Kerangka pemikiran menjelaskan tentang bagaimana teori berhubungan dengan berbagai faktor yang diidentifikasi sebagai masalah yang penting (Sugiyono, 2019). Kerangka pemikiran pada penelitian ini merupakan model konseptual yang didasari oleh *TTAT* yang merupakan sebuah teori penghindaran ancaman yang berhubungan dengan berbagai faktor yang telah diidentifikasi sebagai masalah dalam penelitian. Kerangka pemikiran ditunjukan pada gambar 2.

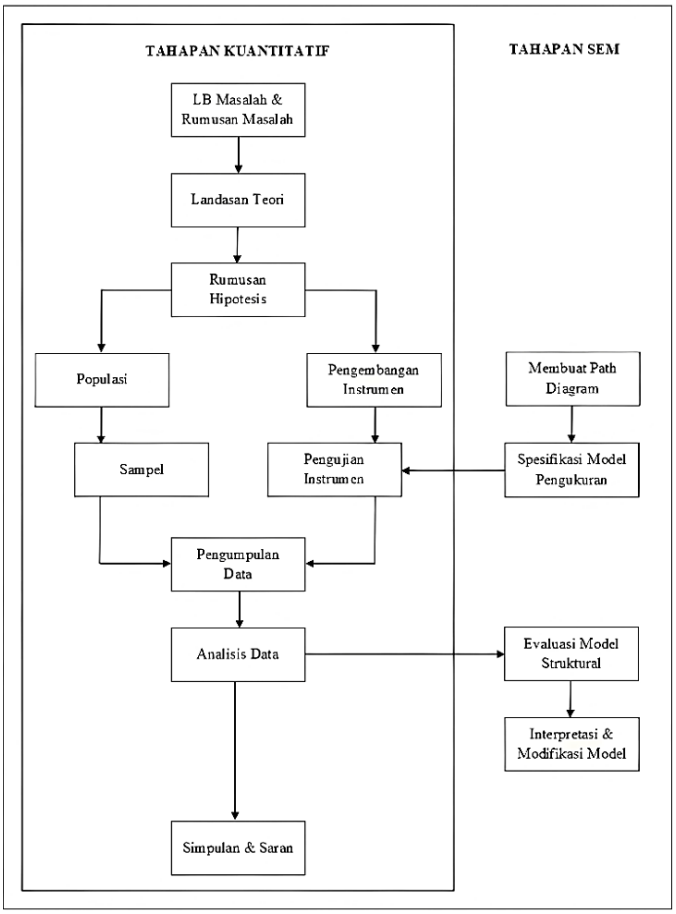


Gambar 2. Kerangka Pemikiran

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

2.3 Tahapan Penelitian

Proses penelitian akan mengikuti metode kuantitatif sebagai tahap utama, kemudian dikombinasikan dengan teknik *Structural Equation Modeling* (*SEM*) untuk analisis data. Tahapan penelitian ditunjukkan pada gambar 3.



Gambar 3. Tahapan Penelitian

Tahapan penelitian yang tunjukkan pada gambar 3 akan dijelaskan lebih lanjut sebagai berikut:

a. Tahap pertama adalah membuat latar belakang dan merumuskan masalah guna menentukan fokus penelitian dengan mengidentifikasi dan merumuskan masalah utama yang ingin diteliti.
b. Tahap kedua adalah menggunakan landasan teori sebagai dasar pemahaman terhadap masalah penelitian.
c. Tahap ketiga yaitu merumuskan hipotesis berdasarkan variabel-variabel TTAT.
d. Tahap keempat yaitu menentukan populasi penelitian dan menghitung jumlah sampel menggunakan rumus slovin, kemudian membagi sampel secara proporsional sesuai populasi.
e. Tahap kelima yaitu mengembangkan instrumen TTAT dan menguji validasi instrumen yang dilakukan oleh 3 ahli serta menguji validitas serta reliabilitas instrumen dengan membuat path diagram dan melakukan spesifikasi model pengukuran dengan teknik CB-SEM menggunakan *tool* SmartPLS 4 untuk memperoleh data yang valid dan akurat.
f. Tahap keenam yaitu melakukan analisis data untuk evaluasi model struktural, interpretasi hasil, dan modifikasi model jika diperlukan dengan teknik CB-SEM.
g. Tahap terakhir yaitu menyimpulkan hasil penelitian dan memberikan rekomendasi berdasarkan hasil analisis dan pembahasan.

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Validitas dan Reliabilitas

Secara umum, total varians yang dapat diterima dari instrumen adalah > 0.50 yang menunjukkan validitas konvergen. Nilai AVE sebesar 0.50 atau lebih tinggi menunjukkan validitas konvergen (Siregar *et al*., 2021). Pada uji validitas konvergen yang dihitung menggunakan *tool* SmartPLS 4, nilai AVE untuk setiap konstruk sudah melebihi 0.50, maka validitas konvergen tercapai. Hasil pengujian validitas dengan validitas konvergen menunjukkan setiap konstruk memiliki nilai *AVE* melebihi 0.5. Nilai *AVE* dapat dilihat pada Tabel 1.

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

Tabel 1. Nilai AVE

	AVE
SUS	0.895
SEV	0.878
THR	0.529
EFF	0.750
COST	0.858
SE	0.852
AM	0.893
AB	0.665

Dalam proses analisis faktor, penelitian ini menetapkan kriteria untuk memilih butir pertanyaan yang valid, dan loading factor yang kurang dari 0.50 dihilangkan (Siregar *et al*., 2021). Penilaian butir pertanyaan yang dihitung menggunakan *tool* SmartPLS 4 menunjukkan semua butir pertanyaan memiliki nilai *loading factor* melebihi 0.50 dan telah lolos uji validitas konvergen. Nilai *loading factor* dapat dilihat pada Tabel 2.

Tabel 2. Nilai Loading Factor

	SUS	SEV	THR	EFF	COST	SE	AM	AB
SUS1	0.961							
SUS4	0.910							
SUS5	0.966							
SEV2		0.855						
SEV5		0.975						
SEV6		0.957						
SEV7		0.956						
THR1			0.616					
THR2			0.713					
THR3			0.816					
THR4			0.738					
THR5			0.739					
EFF1				0.976				
EFF2				0.765				
EFF3				0.748				
EFF4				0.951				
COST1					0.994			
COST2					0.841			
COST3					0.937			
SE1						0.936		
SE2						0.912		
SE3						0.921		
SE7						0.933		
SE8						0.912		
AM1							0.974	
AM2							0.908	
AM3							0.951	
AB1								0.754
AB2								0.872

Validitas diskriminan ditetapkan artinya setiap konstruk mampu menangkap fenomena unik yang tidak diwakilkan oleh konstruk lain dalam model (Siregar *et al*., 2021). Penilaian validitas diskriminan dengan kriteria Fornell-Larcker, yaitu dengan membandingkan Akar kuadrat AVE > Korelasi antar Konstruk Laten. Hasil pengujian validitas dengan validitas diskriminan yang dihitung menggunakan *tool* SmartPLS 4 menunjukkan nilai akar kuadrat AVE dari kriteria fornell-larcker sudah lebih besar dari korelasi antar konstruk laten. Nilai fornell-larcker ditunjukkan pada Tabel 3.

Tabel 3. Nilai Fornell-larcker

	AB	AM	COST	EFF	SE	SEV	SUS	THR
AB	0.815							
AM	0.813	0.945						
COST	-0.026	-0.127	0.926					
EFF	-0.048	-0.105	-0.084	0.720				

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

	AB	AM	COST	EFF	SE	SEV	SUS	THR
SE	0.219	0.070	0.351	-0.058	0.672			
SEV	-0.106	-0.065	0.081	0.261	-0.108	0.645		
SUS	0.151	0.038	-0.076	0.217	-0.160	0.260	0.747	
THR	0.099	-0.025	-0.097	0.632	-0.104	0.433	0.582	0.727

Kedua, pengujian reliabilitas instrumen. Untuk memenuhi CB-SEM, Siregar *et al*. (2021) menyarankan bahwa *Cronbach's α* > 0,60 dapat digunakan sebagai indeks untuk mengkonfirmasi konsistensi internal dari suatu pengukuran. *Composite Reliability* > 0.70, menunjukkan bahwa pengukuran dalam studi ini dapat diandalkan (Siregar *et al*., 2021). Hasil pengujian reliabilitas dengan *Cronbach's* α dan *Composite Reliability* yang dihitung menggunakan *tool* SmartPLS 4 menunjukkan nilai *Cronbach's* α melebihi 0,60 serta *Composite Reliability* melebihi 0.70. Dengan demikian, instrumen penelitian yang digunakan telah terbukti valid dan reliabel. Nilai konstruk reliabilitas ditunjukkan pada Tabel 4.

Tabel 4. Nilai Konstruk Reliabilitas

	Cronbach's α	*Composite Reliability*
SUS	0.962	0.962
SEV	0.965	0.966
THR	0.844	0.848
EFF	0.931	0.930
COST	0.944	0.949
SE	0.966	0.966
AM	0.961	0.961
AB	0.793	0.795

3.2 Pengujian Model Fit

Setelah instrumen penelitian terbukti valid dan reliabel, tahap selanjutnya adalah melakukan evaluasi terhadap model guna memastikan bahwa konstruk atau variabel yang digunakan sesuai dan layak (*fit*) dengan model yang dibangun (Siregar *et al*., 2021). Secara keseluruhan, *Goodness of Fit* dinilai berdasarkan lima kriteria, namun peneliti tidak wajib memenuhi semuanya karena keputusan akhir bergantung pada penilaian masing-masing peneliti.
Berdasarkan hasil pengujian *Goodness of Fit* terhadap model yang dihitung menggunakan *tool* SmartPLS 4, dapat disimpulkan bahwa model layak digunakan karena telah memenuhi dua indikator utama *Goodness of Fit*, yaitu nilai Chi-Square/df dan RMSEA yang berada dalam batas rekomendasi. Rincian hasil kelayakan model disajikan pada Tabel 5.

Tabel 5. Output Model Fit

Fit Indices	*Recommended Value*	*Value*
Chi-Square/df	<= 2	1.549
RMSEA	<= 0.08	0.074
GFI	>= 0.90	0.749
AGFI	>= 0.90	0.687
SRMR	<= 0.05	0.058

3.3 Hasil Penelitian

Penelitian ini memiliki sembilan hipotesis yang akan diuji melalui model struktural dengan mengevaluasi nilai *path coefficient*. Kriteria evaluasi meliputi: arah nilai *parameter estimates* (positif atau negatif) dan P value < 0,050 yang menunjukkan pengaruh signifikan dengan tingkat kepercayaan 95% (Siregar *et al*., 2021). Hasil uji hipotesis yang dihitung menggunakan *tool* SmartPLS 4 ditunjukkan pada tabel 6.

Tabel 6. Output Path Coefficient

	Parameter Estimates (β)	P Values
H1a : SUS -> THR	0.247	0.000
H1b : SEV -> THR	0.169	0.000
H1c : SUSxSEV -> THR	0.043	0.034
H2 : THR -> AM	0.178	0.019
H3 : EFF -> AM	-0.009	0.741
H3a : THRxEFF -> AM	-0.120	0.001
H4 : COST -> AM	-0.009	0.713
H5 : SE -> AM	0.063	0.020
H6 : AM -> AB	0.770	0.000

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

Berdasarkan hasil perhitungan menggunakan algoritma CB-SEM dengan melihat nilai *path coefficient*, berikut adalah penjelasan hasil pengujian hipotesis dari Tabel 6.

a. *Perceived susceptibility* berpengaruh positif signifikan terhadap *perceived threat* (β = 0.247; p-value 0.000 < 0.05). Dengan demikian, hipotesis H1a diterima.
b. *Perceived severity* berpengaruh positif signifikan terhadap *perceived threat* (β = 0.169; p-value 0.000 < 0.05). Dengan demikian, hipotesis H1b diterima.
c. Interaksi antara *perceived susceptibility* dan *perceived severity* berpengaruh positif signifikan terhadap *perceived threat* (β = 0.043; p-value 0.034 < 0.05). Oleh karena itu, hipotesis H1c diterima.
d. *Perceived threat* berpengaruh positif dan signifikan terhadap *avoidance motivation* (β = 0.178; p value 0.019 < 0.05), sehingga hipotesis H2 diterima.
e. *Safeguard effectiveness* tidak berpengaruh signifikan terhadap *avoidance motivation* (β = -0.009; p value = 0.741 > 0.05), sehingga hipotesis nol (Ho) pada H3 diterima.
f. Interaksi antara *perceived threat* dan *safeguard effectiveness* berpengaruh negatif dan signifikan terhadap *avoidance motivation* (β = -0.120; p value = 0.001 < 0.05), sehingga hipotesis H3a diterima.
g. *Safeguard cost* tidak berpengaruh signifikan terhadap *avoidance motivation* (β = -0.009; p value = 0.713 > 0.05), sehingga hipotesis nol (Ho) pada H4 diterima.
h. *Self-efficacy* berpengaruh positif dan signifikan terhadap *avoidance motivation* (β = 0.063; p value = 0.020 < 0.05), sehingga hipotesis H5 diterima.
i. *Avoidance motivation* berpengaruh positif dan signifikan terhadap *avoidance behavior* (β = 0.770; p value = 0.000 < 0.05), sehingga hipotesis H6 diterima.

3.4 Pembahasan

Berdasarkan hasil penelitian, berikut adalah pembahasan mengenai hasil pengujian hipotesis.

a. Persepsi kerentanan berpengaruh positif signifikan terhadap persepsi ancaman, yang sejalan dengan temuan (Carpenter *et al*., 2019; Mark *et al*., 2021; Saidi & Prayudi, 2021; Sylvester, 2022) yang juga menunjukkan hubungan positif antara persepsi kerentanan dan persepsi ancaman. Pengguna SIMAK yang merasa privasi data mereka terancam cenderung merespons ancaman dengan serius. Hal ini menegaskan pentingnya memperhatikan persepsi kerentanan dalam merancang pengamanan efektif guna meningkatkan kewaspadaan terhadap privasi data.
b. Persepsi keparahan berpengaruh positif terhadap persepsi ancaman, sesuai dengan temuan (Carpenter *et al*., 2019; Mark *et al*., 2021; Saidi & Prayudi, 2021; Sylvester, 2022) yang juga mengonfirmasi pengaruh positif tersebut. Pengguna SIMAK yang menilai konsekuensi ancaman privasi data sangat merugikan cenderung menganggap ancaman tersebut lebih serius. Persepsi keparahan memperkuat persepsi ancaman, karena semakin besar keparahan yang dirasakan, semakin tinggi kesadaran individu terhadap bahaya yang mengancam privasi data mereka.
c. Interaksi antara persepsi kerentanan dan keparahan berpengaruh positif terhadap persepsi ancaman. Temuan ini sejalan dengan penelitian (Sylvester, 2022) yang juga mengungkapkan bahwa interaksi kedua persepsi tersebut memengaruhi persepsi ancaman secara signifikan. Pengguna SIMAK yang merasa rentan terhadap ancaman privasi data dan menganggap konsekuensinya parah cenderung merasakan ancaman tersebut lebih signifikan. Kombinasi kedua persepsi ini mendorong kesadaran ancaman, sehingga mereka lebih waspada dalam melindungi privasi data di SIMAK.
d. Persepsi ancaman berpengaruh positif terhadap motivasi menghindari ancaman keamanan pribadi. Temuan ini sesuai dengan penelitian (Mark *et al*., 2021) yang menyatakan bahwa persepsi ancaman secara langsung meningkatkan motivasi pengguna untuk menghindari risiko dan ancaman. Pengguna SIMAK yang merasa ancaman signifikan terhadap privasi data mereka cenderung termotivasi untuk menghindari risiko dengan melakukan tindakan pengamanan lebih kuat atau menghindari aktivitas berisiko. Semakin besar persepsi ancaman, semakin tinggi kecenderungan mereka untuk mengambil langkah penghindaran.
e. Efektivitas pengamanan tidak berpengaruh terhadap motivasi untuk menghindari ancaman keamanan pribadi. Temuan ini berbeda dengan hasil studi (Butler, 2020) yang menyatakan efektivitas pengamanan berpengaruh positif terhadap motivasi penghindaran. Perbedaan tersebut kemungkinan disebabkan oleh karakteristik pengguna SIMAK dalam penelitian ini, yang menganggap langkah pengamanan seperti pembaruan kata sandi terlalu sederhana. Peretas masih memiliki banyak cara untuk mencuri kata sandi atau meretas akun (Rifai *et al*., 2023). Oleh karena itu, pengguna SIMAK merasa bahwa pembaruan kata sandi tidak cukup efektif untuk memengaruhi motivasi mereka dalam menghindari ancaman. Meskipun pengguna SIMAK memahami cara updating password, mereka menilai langkah ini kurang efektif, sehingga tidak berpengaruh signifikan terhadap motivasi mereka untuk menghindari ancaman. Akibatnya, motivasi penghindaran mereka menjadi rendah.
f. Interaksi antara persepsi ancaman dan efektivitas pengamanan berpengaruh negatif terhadap motivasi untuk menghindari ancaman privasi data. Temuan ini konsisten dengan penelitian (Sylvester, 2022) yang menemukan efek interaksi negatif antara persepsi ancaman dan efektivitas pengamanan terhadap motivasi penghindaran. Semakin tinggi persepsi ancaman pengguna, jika langkah pengamanan seperti updating password dinilai efektif, motivasi mereka untuk menghindari ancaman justru menurun. Artinya, pengguna yang merasa terancam tapi percaya pengamanan sudah cukup efektif kurang terdorong mengambil tindakan penghindaran lebih lanjut.
g. Biaya pengamanan tidak berpengaruh terhadap motivasi untuk menghindari ancaman privasi data. Temuan ini konsisten dengan temuan (Arachchilage & Love, 2014) yang juga menghasilkan biaya pengamanan tidak

TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

memengaruhi motivasi penghindaran. Pengguna SIMAK menganggap biaya updating password rendah dan langkah ini sederhana (Raharjo, 2021), sehingga mereka tidak memikirkan atau mempertimbangkan biaya tersebut.

h. Efikasi diri berpengaruh positif terhadap motivasi untuk menghindari ancaman privasi data. Temuan ini konsisten dengan penelitian (Gillam & Foster, 2020; Mark *et al*., 2021; Saidi & Prayudi, 2021; Tang *et al*., 2021; Verkijika, 2019) yang menyatakan bahwa efikasi diri meningkatkan motivasi pengguna dalam menghindari ancaman. Semakin tinggi keyakinan pengguna SIMAK dalam kemampuan updating password, semakin besar motivasi mereka untuk menghindari ancaman privasi data. Keyakinan diri ini mendorong tindakan pencegahan yang lebih proaktif menghadapi risiko keamanan.

i. Motivasi penghindaran berpengaruh positif terhadap perilaku kesadaran dalam menghindari ancaman privasi data. Temuan ini sejalan dengan studi (Butler, 2020; Gillam & Foster, 2020; Mark *et al*., 2021; Rifai *et al*., 2023; Saidi & Prayudi, 2021; Sylvester, 2022; Verkijika, 2019), yang mengonfirmasi peran penting motivasi penghindaran dalam mendorong perilaku pengguna untuk menghindari ancaman. Semakin tinggi motivasi pengguna SIMAK untuk menghindari ancaman, semakin besar pula kesadaran mereka dalam melindungi privasi data melalui tindakan nyata, seperti menggunakan kata sandi kuat. Motivasi ini juga membantu membangun kesadaran kolektif untuk menciptakan budaya keamanan data yang lebih baik di lingkungan SIMAK.

4. KESIMPULAN

Berdasarkan hasil penelitian, ditemukan bahwa sebagian besar variabel dalam model memiliki pengaruh signifikan. Persepsi kerentanan, keparahan, efikasi diri, serta persepsi ancaman terbukti memiliki pengaruh terhadap motivasi pengguna untuk menghindari ancaman terhadap privasi data, yang pada akhirnya berdampak pada perilaku nyata dalam menjaga keamanan privasi data mereka. Namun, efektivitas dan biaya pengamanan tidak berpengaruh signifikan terhadap motivasi menghindari ancaman privasi data, mengindikasikan bahwa pengguna SIMAK memandang langkah pengamanan yang ada saat ini belum cukup kuat atau terlalu sederhana untuk diandalkan sepenuhnya dalam mengamankan privasi data. Interaksi antar variabel juga berperan penting membentuk persepsi dan motivasi pengguna terhadap ancaman privasi data. Keseluruhan hasil ini menegaskan bahwa kesadaran pengguna terhadap privasi data sangat dipengaruhi oleh faktor psikologis seperti persepsi ancaman dan efikasi diri. Dengan demikian, sangat penting bagi pengelola SIMAK untuk menyusun strategi untuk mengurangi ancaman yang lebih efektif, seperti menyempurnakan kebijakan keamanan. Adapun keterbatasan dalam penelitian ini adalah konteksnya yang terbatas pada sistem informasi akademik di lingkungan UIN Raden Fatah saja, sehingga hasilnya belum tentu dapat digeneralisasi ke sistem informasi lain atau sektor yang berbeda. Selain itu, penelitian ini belum menguji variabel-variabel eksternal lain yang mungkin relevan, seperti yang terdapat dalam *Protection Motivation Theory (PMT)*. Oleh karena itu, disarankan agar penelitian berikutnya melibatkan integrasi variabel tambahan guna mengevaluasi pengaruhnya terhadap perilaku pengguna dalam menjaga privasi data.

REFERENCES

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/https://doi.org/10.1016/j.chb.2014.05.046

Butler, R. (2020). A systematic literature review of the factors affecting smartphone user threat avoidance behaviour. *Information and Computer Security*, *28*(4), 555–574. https://doi.org/10.1108/ICS-01-2020-0016/FULL/XML

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*(1), 380–407. https://doi.org/10.17705/1CAIS.04422

Djatsa, F. (2020). Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations. *Journal of Information Security*, *11*(1), 19–45. https://doi.org/10.4236/JIS.2020.111002

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, *108*, 106319. https://doi.org/10.1016/J.CHB.2020.106319

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, Journal of the Association for Information Systems , *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Machali, I. (2021). *Metode Penelitian Kuantitatif Panduan Praktis Merencanakan, Melaksanakan dan Analisis dalam Penelitian Kuantitatif* (A. Q. Habib, Ed.). Yogyakarta: Fakultas Ilmu Tarbiyah dan Keguruan.

Mark, M. S., Borda, O., Stroman, J., Member, C., & Wilson, T. C. (2021). *An Analysis of Factors Influencing Phising Threat Avoidance Behaviour: A Quantitative Study*.

Raharjo, B. (2021). *Keamanan Sistem Informasi* (M. C. Wibowo, Ed.). Semarang: Yayasan Prima Agus Teknik.

Ramayani, Y., Oktarina, T., (2022). *Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)*. Jurnal Inovtek, *7*(2), 289–296. https://doi.org/http://dx.doi.org/10.35314/isi.v7i2.2631


TIN: Terapan Informatika Nusantara
Vol 6, No 1, June 2025, page 24-33
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i1.7590

Razzaq, A., Aditya, M., Widya, A., Kuncoro Putri, O., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*. https://doi.org/10.34010/gpsjournal.v6i1

Rifai, A., Meliyani, A., Chyntia, P., & Sakti, I. A. (2023). Penerapan Metode Technology Threat Avoidance Theory Terhadap Tingkat Kesadaran Data Privasi Pengguna Media Sosial. *Journal of Information System Research (JOSH)*, *4*(3), 1026–1032. https://doi.org/10.47065/josh.v4i3.3081

Saidi, K., & Prayudi, Y. (2021). *Analisis Indikator Utama Dalam Information Security-Personality Threat Terhadap Phishing Attack Menggunakan Metode Technology Threat Avoidance Theory (TTAT)*. Justindo. https://doi.org/http://dx.doi.org/10.32528/justindo.v6i1.3801

Siregar, Z. M. E., Parlaungan, A., Supriadi, Y. N., Ende, & Pristiyono. (2021). *Structural Equation Modeling Konsep dan Implementasinya pada Kajian Ilmu Manajemen dengan Menggunakan AMOS*. Yogyakarta: Deepublish.

Sugiyono. (2019). *Metode Penelitian Kuantitatif* (Setiyawami, Ed.). Bandung: Alfabeta.

Sylvester, F. L. (2022). Mobile Device Users' Susceptibility to Phishing Attacks. *International Journal of Computer Science and Information Technology*, *14*(1), 1–18. https://doi.org/10.5121/ijcsit.2022.14101

Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, *38*(2), 101572. https://doi.org/10.1016/J.GIQ.2021.101572

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286–296. https://doi.org/10.1016/J.CHB.2019.07.034

Waluyo, M., & Rachman, M. (2020). *Mudah Cepat Tepat Dalam Aplikasi Structural Equation Modeling* (N. A. Rahma, Ed.). Malang: Literasi Nusantara.