

KEKHAWATIRAN PRIVASI DATA DAN KEPERCAYAAN PENGGUNA MOBILE JKN PASCA KEBOCORAN DATA BPJS KESEHATAN: PERSPEKTIF *PROTECTION MOTIVATION THEORY*

Miranda Pakpahan¹, Dewi Lestari², Rudi Nata³

^{1,2,3}Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Jambi
Jl. Jambi - Muara Bulian No.KM. 15, Kabupaten Muaro Jambi, Jambi, telp.081273574983
e-mail: ¹mirandapakpahan36@gmail.com , ²dewilestari@unja.ac.id , ³rudinata@unja.ac.id

Abstrak

Kebocoran data BPJS Kesehatan pada tahun 2021 yang diduga melibatkan sekitar 279 juta data penduduk Indonesia menimbulkan pertanyaan mengenai bagaimana persepsi risiko privasi memengaruhi niat pengguna untuk tetap menggunakan aplikasi Mobile JKN. Penelitian ini bertujuan menganalisis pengaruh *perceived severity*, *perceived vulnerability*, *response efficacy*, *self-efficacy*, *response cost*, *privacy concern*, dan *trust* terhadap *Behavioral intention* pengguna Mobile JKN dengan pendekatan *Protection Motivation Theory* (PMT) yang diperluas. Data dikumpulkan dari 210 responden pengguna Mobile JKN di Indonesia melalui kuesioner daring dan dianalisis menggunakan metode *Partial Least Square Structural Equation Modeling* (PLS-SEM) dengan bantuan *SmartPLS 4*. Hasil penelitian menunjukkan bahwa *Perceived vulnerability* berpengaruh negatif dan signifikan, sedangkan *trust* berpengaruh positif dan signifikan terhadap *Behavioral intention*, dengan *trust* sebagai faktor paling dominan dalam model, sedangkan *perceived severity*, *response efficacy*, *self-efficacy*, *response cost*, dan *privacy concern* tidak terbukti berpengaruh signifikan. Penelitian ini diharapkan dapat memberikan kontribusi teoretis bagi pengembangan model PMT pada konteks layanan publik digital, serta kontribusi praktis bagi BPJS Kesehatan dalam merumuskan strategi peningkatan keamanan dan kepercayaan pengguna terhadap Mobile JKN.

Kata kunci: *Protection Motivation Theory*, *Privacy Concern*, *Trust*, Mobile JKN, kebocoran data, PLS-SEM

Abstract

The 2021 BPJS Kesehatan data breach, allegedly involving approximately 279 million records of Indonesian citizens, raised questions regarding how privacy risk perceptions influence users' intention to continue using the Mobile JKN application. This study aimed to analyze the influence of perceived severity, perceived vulnerability, response efficacy, self-efficacy, response cost, privacy concern, and trust on the Behavioral intention of Mobile JKN users through an extended Protection Motivation Theory (PMT) approach. Data were collected from 210 Mobile JKN users in Indonesia through an online questionnaire and analyzed using the Partial Least Square Structural Equation Modeling (PLS-SEM) method with the aid of SmartPLS 4. The results showed that Perceived vulnerability had a significant negative effect, while trust had a significant positive effect on Behavioral intention, with trust being the most dominant factor in the model, whereas perceived severity, response efficacy, self-efficacy, response cost, and privacy concern were not found to have a significant effect. This study is expected to provide theoretical contributions to the development of the PMT model in the context of public digital services, as well as practical contributions to BPJS Kesehatan in formulating strategies to enhance security and user trust in the Mobile JKN application.

Keywords: *Protection Motivation Theory*, *Privacy Concern*, *Trust*, Mobile JKN, data breach, PLS-SEM

1. PENDAHULUAN

Sebagai bentuk inovasi layanan berbasis teknologi informasi, BPJS Kesehatan menghadirkan aplikasi Mobile JKN yang memungkinkan pasien rumah sakit mengakses berbagai layanan kesehatan secara

lebih mudah, termasuk pendaftaran secara daring, pengecekan ketersediaan kamar rawat inap, serta sejumlah fitur pendukung lainnya [1]. Dengan jumlah peserta JKN yang mencapai lebih dari 283 juta per November 2025, ketergantungan masyarakat terhadap layanan digital ini sangat tinggi. Sebagai aplikasi yang mengelola informasi kepesertaan dan data pribadi yang bersifat sensitif, Mobile JKN menempatkan aspek keamanan dan perlindungan privasi sebagai faktor penting dalam menjaga kepercayaan pengguna [2].

Urgensi isu keamanan data semakin meningkat sejak munculnya dugaan kebocoran data BPJS Kesehatan pada tahun 2021 yang melibatkan sekitar 279 juta data penduduk Indonesia. Data yang diduga bocor mencakup informasi sensitif, seperti nama lengkap, Nomor Induk Kependudukan (NIK), nomor telepon, alamat, dan alamat email [3]. Data tersebut diduga diperjualbelikan secara ilegal di forum daring menggunakan mata uang kripto, meskipun pemerintah melalui Kementerian Komunikasi dan Informatika masih melakukan penelusuran untuk memastikan sumber, jumlah, dan validitas data tersebut [4]. Insiden ini menunjukkan bahwa kelemahan sistem keamanan dapat meningkatkan risiko pencurian identitas, penipuan digital, serta menurunkan kepercayaan masyarakat terhadap keamanan sistem informasi publik [5].

Persoalan utama dalam penelitian ini bukan sekadar terjadinya kebocoran data, melainkan bagaimana persepsi pengguna terhadap risiko tersebut membentuk *Behavioral intention* untuk tetap menggunakan Mobile JKN pascakebocoran data BPJS Kesehatan. Untuk memperoleh gambaran awal mengenai fenomena ini, peneliti melakukan pra-survei melalui kuesioner daring terhadap 30 pengguna aktif Mobile JKN. Hasil pra-survei menunjukkan bahwa sebanyak 70% responden mengetahui adanya kebocoran data BPJS Kesehatan tahun 2021. Dari kelompok tersebut, 66,7% menyatakan tetap menggunakan aplikasi, 13,3% sempat berhenti kemudian kembali menggunakan, dan hanya 20% yang benar-benar berhenti menggunakan Mobile JKN. Temuan ini menunjukkan bahwa mayoritas pengguna tetap memanfaatkan aplikasi meskipun menyadari adanya risiko kebocoran data. Penelusuran terhadap ulasan pengguna di *Google Play Store* juga memperlihatkan bahwa kekhawatiran terhadap keamanan data masih muncul secara konsisten, bahkan pada pengguna yang memberikan penilaian positif terhadap aplikasi. Fenomena ini mengindikasikan bahwa penggunaan Mobile JKN belum tentu mencerminkan tingginya rasa aman atau kepercayaan, melainkan dapat dipengaruhi oleh tidak tersedianya layanan kesehatan digital yang setara [6].

Fenomena tersebut mengindikasikan bahwa insiden kebocoran data tidak hanya meningkatkan *privacy concern*, tetapi juga berpotensi memengaruhi *Trust* pengguna terhadap kemampuan BPJS Kesehatan dalam melindungi informasi pribadi mereka. *Privacy Concern* menggambarkan tingkat kekhawatiran pengguna terhadap pengumpulan, penyimpanan, akses, dan potensi penyalahgunaan data pribadi [7], sedangkan *Trust* berkaitan dengan keyakinan bahwa penyedia layanan mampu mengelola data secara aman, andal, dan bertanggung jawab [8]. Kedua faktor tersebut diduga berperan penting dalam membentuk *Behavioral intention* pengguna untuk tetap menggunakan Mobile JKN setelah terjadinya kebocoran data.

Untuk menjelaskan fenomena tersebut, penelitian ini menggunakan *Protection Motivation Theory* (PMT) yang menjelaskan proses kognitif individu dalam menilai ancaman serta menentukan respons perlindungan yang akan diambil [9]. Dalam kerangka PMT, penilaian ancaman tercermin dari *perceived severity*, yaitu persepsi individu terhadap tingkat keseriusan dampak yang ditimbulkan apabila data pribadinya disalahgunakan, serta *Perceived vulnerability*, yaitu persepsi individu mengenai seberapa besar kemungkinan dirinya menjadi korban dari risiko tersebut. Adapun penilaian koping tercermin dari *response efficacy*, yaitu keyakinan bahwa tindakan perlindungan yang diambil akan efektif mengurangi risiko; *self-efficacy*, yaitu keyakinan individu terhadap kemampuannya sendiri dalam melakukan tindakan perlindungan data; serta *response cost*, yaitu persepsi mengenai besarnya usaha, waktu, atau hambatan yang harus dikeluarkan untuk melakukan tindakan perlindungan tersebut [10]. Kelima konstruk ini kemudian diperluas dengan menambahkan *Privacy Concern* dan *Trust* sebagai variabel tambahan terhadap *Behavioral intention*.

Pendekatan serupa telah diterapkan pada konteks aplikasi komersial, seperti *App Tracking Transparency* [11] dan aplikasi perbankan digital SeaBank [12]. Namun, penelitian-penelitian tersebut berfokus pada layanan yang bersifat opsional, di mana pengguna memiliki keleluasaan untuk berpindah atau berhenti menggunakan layanan apabila merasa dirugikan. Kondisi ini berbeda dengan Mobile JKN yang merupakan layanan kesehatan publik nasional dengan tingkat kebutuhan yang jauh lebih tinggi

karena keterkaitannya langsung dengan akses jaminan kesehatan masyarakat. Hingga saat ini, penelitian yang mengintegrasikan PMT dengan *Privacy Concern* dan *Trust* secara khusus pada konteks layanan kesehatan digital publik seperti Mobile JKN pascakebocoran data BPJS Kesehatan masih sangat terbatas. Kebaruan (*novelty*) penelitian ini terletak pada pengujian model PMT yang diperluas dalam konteks layanan publik yang sangat dibutuhkan, yang secara karakteristik berbeda dari layanan komersial opsional yang banyak diteliti sebelumnya.

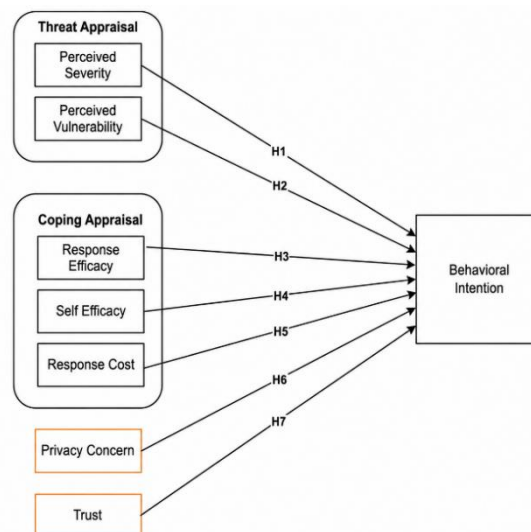
Berdasarkan uraian tersebut, rumusan masalah dalam penelitian ini adalah bagaimana pengaruh *perceived severity*, *Perceived vulnerability*, *response efficacy*, *self-efficacy*, *response cost*, *privacy concern*, dan *Trust* terhadap *Behavioral intention* pengguna Mobile JKN pascakebocoran data BPJS Kesehatan. Oleh karena itu, penelitian ini bertujuan menganalisis pengaruh ketujuh variabel tersebut terhadap *Behavioral intention* pengguna Mobile JKN, sehingga diharapkan dapat memberikan kontribusi teoretis bagi pengembangan model PMT pada konteks layanan publik, serta kontribusi praktis bagi BPJS Kesehatan dalam merumuskan strategi peningkatan keamanan dan kepercayaan pengguna terhadap Mobile JKN.

2. METODE PENELITIAN

Dalam penelitian ini dipilih pendekatan kuantitatif, di mana metode deskriptif digunakan untuk memberikan gambaran umum, sedangkan metode eksplanatori dipakai untuk menguji keterkaitan antarvariabel. Metode deskriptif dipakai untuk menggambarkan kondisi aktual terkait kekhawatiran privasi data, persepsi ancaman, dan kepercayaan pengguna dalam menggunakan aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan, sedangkan metode eksplanatori digunakan untuk menelaah hubungan antarvariabel dalam kerangka *Protection Motivation Theory* (PMT) melalui analisis *Structural Equation Modeling-Partial Least Square* (SEM-PLS) menggunakan SmartPLS 4. Evaluasi model dilakukan dengan mengintegrasikan uji model pengukuran (*outer model*) yang meliputi uji validitas dan reliabilitas, serta uji model struktural (*inner model*) yang meliputi R-Square, F-Square, Q-Square, dan uji hipotesis dengan *bootstrapping* signifikansi jalur (*path coefficient*).

2.1. Model dan Hipotesis Penelitian

Model teoritis dalam penelitian ini didasarkan pada *Protection Motivation Theory* (PMT) yang dikembangkan oleh Rogers (1983) mencakup variabel independen (bebas), yaitu Persepsi Keseriusan (*Perceived severity*), Persepsi kerentanan (*Perceived vulnerability*), Efektivitas Tindakan (*Response efficacy*), Efektivitas Diri (*Self-Efficacy*), Biaya Respons (*Response cost*), PMT diperluas dengan menambahkan variabel *Privacy Concern* (kekhawatiran privasi) dan *Trust* (kepercayaan). Fokus penelitian diarahkan pada variabel-variabel yang memiliki keterkaitan kuat dengan *Behavioral intention* (niat perilaku) [13]. Dengan demikian, kerangka pemikiran penelitian dirumuskan ke dalam model konseptual sebagai berikut.



Gambar 1. Model Penelitian

Tabel 1. Hipotesis Penelitian

Kode Hipotesis	Rumusan Hipotesis
H1	<i>Perceived severity</i> berpengaruh negatif terhadap <i>Behavioral intention</i> pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.
H2	<i>Perceived vulnerability</i> berpengaruh negatif terhadap <i>Behavioral intention</i> pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.
H3	<i>Response Efficacy</i> berpengaruh positif terhadap <i>Behavioral intention</i> pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.
H4	Self efficacy berpengaruh positif terhadap <i>Behavioral intention</i> pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.
H5	<i>Response Cost</i> berpengaruh negatif terhadap <i>Behavioral intention</i> pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.
H6	<i>Privacy Concern</i> berpengaruh negatif terhadap <i>Behavioral intention</i> pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.
H7	<i>Trust</i> berpengaruh positif terhadap <i>Behavioral intention</i> pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.

2.2. Populasi, Sampel, dan Pengumpulan Data

Populasi dalam penelitian ini adalah seluruh masyarakat di Indonesia yang menggunakan aplikasi Mobile JKN sebagai objek studi, mencakup keseluruhan pengguna aktif aplikasi tersebut yang dianggap mewakili kelompok pengguna Mobile JKN secara nasional. Karena jumlah pasti pengguna yang mengetahui dan terdampak isu kebocoran data BPJS Kesehatan tidak diketahui secara pasti (*unknown population*), penelitian ini menggunakan teknik *non-probability sampling*, yakni teknik pengambilan sampel di mana tidak semua anggota populasi memiliki peluang yang sama untuk terpilih menjadi responden, dan pemilihan sampel didasarkan pada pertimbangan subjektif peneliti sesuai kriteria tertentu [14]. Penentuan sampel dilakukan secara *purposive sampling*, yakni memilih responden yang telah memenuhi kriteria, yaitu merupakan pengguna aplikasi Mobile JKN di Indonesia, berusia minimal 17 tahun, dan mengetahui informasi mengenai insiden kebocoran data BPJS Kesehatan tahun 2021. Ukuran sampel ditentukan menggunakan pedoman Hair et al.[15], yang menyatakan bahwa jumlah sampel minimum dalam analisis SEM-PLS adalah 5 hingga 10 kali jumlah indikator yang digunakan. Penelitian ini menggunakan 21 indikator, sehingga jumlah sampel minimum dihitung sebagai berikut: Sampel = $21 \times 10 = 210$ responden. Pendekatan Hair et al. dipilih karena populasi penelitian bersifat tidak diketahui jumlahnya secara pasti, sehingga rumus berbasis jumlah indikator lebih sesuai dibandingkan rumus berbasis proporsi populasi seperti Slovin. Dengan demikian, jumlah sampel minimum yang ditetapkan dalam penelitian ini adalah sebanyak 210 responden pengguna aplikasi Mobile JKN di Indonesia.

2.3. Penyusunan Instrumen Penelitian

Penelitian ini mengadaptasi indikator dari penelitian sebelumnya yang relevan, contohnya penelitian [16] dan [17]. Penelitian ini menggunakan lima variabel yang dianalisis dan dioperasionalkan berdasarkan kerangka *Protection Motivation Theory* (PMT). Selain itu, penelitian ini juga mengoperasionalkan dua variabel tambahan yang relevan dalam konteks keamanan dan privasi digital, yaitu *Privacy Concern* dan *Trust*, karena keduanya memiliki peran strategis dalam membentuk intensi perilaku (*Behavioral intention*) pengguna untuk tetap menggunakan aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan 2021. Skala pengukuran yang digunakan dalam penelitian ini adalah skala likert 4 point. Secara keseluruhan, ketujuh variabel tersebut diukur menggunakan 21 indikator penelitian, yang telah disusun dan disajikan secara sistematis dalam tabel operasional variabel berikut ini.

Tabel 2. Instrumen Penelitian

Variabel	Indikator/Pernyataan	Kode	Referensi
Persepsi keseriusan (<i>Perceived severity</i>)	Kebocoran data BPJS Kesehatan dapat menimbulkan dampak yang serius bagi saya sebagai pengguna Mobile JKN.	PS1	(Vance et al., 2012)
	Kebocoran data BPJS Kesehatan merupakan ancaman serius terhadap keamanan data pribadi saya.	PS 2	(Rogers W., 1983)
Persepsi kerentanan (<i>Perceived vulnerability</i>)	Saya merasa data pribadi saya dapat mengalami kebocoran di aplikasi Mobile JKN.	PV1	(Workman et al., 2008)
	Saya menilai data pribadi saya di aplikasi Mobile JKN berpotensi diakses oleh pihak yang tidak berwenang.	PV2	(Rogers, 1975)
	Saya merasa terdapat risiko terjadinya pelanggaran keamanan data terhadap informasi pribadi saya di Mobile JKN.	PV3	
Efektivitas respon (<i>Response efficacy</i>)	Menjaga informasi pribadi dengan baik dapat mencegah penyalahgunaan data pada aplikasi Mobile JKN.	RE1	(Xiao et al., 2014)
	Mengikuti langkah-langkah keamanan pada aplikasi Mobile JKN dapat mengurangi risiko kebocoran data.	RE2	
	Memperbarui kata sandi dan menjaga keamanan akun dapat mencegah akses tidak sah ke akun Mobile JKN.	RE3	
Keyakinan diri (<i>Self efficacy</i>)	Bagi saya, menjaga keamanan data pada aplikasi Mobile JKN merupakan hal yang mudah dilakukan.	SE1	(Workman et al., 2008)
	Saya mampu menggunakan langkah-langkah keamanan yang tersedia untuk mencegah orang lain mengakses data pribadi saya di aplikasi Mobile JKN.	SE2	(Rogers, 1975)
	Saya memiliki kemampuan untuk menjaga akun Mobile JKN saya agar tidak diakses oleh pihak lain tanpa izin.	SE3	
Biaya Respon (<i>Response costs</i>)	Bagi saya, menerapkan langkah-langkah keamanan data pada aplikasi Mobile JKN terasa merepotkan.	RC1	(Hassani et al., 2014)
	Saya merasa tidak nyaman karena harus melakukan tindakan keamanan secara berulang, seperti mengganti kata sandi pada aplikasi Mobile JKN.	RC2	
Kekhawatiran Privasi (<i>Privacy concern</i>)	Saya khawatir data pribadi saya pada aplikasi Mobile JKN dapat disalahgunakan untuk tujuan yang tidak semestinya.	PC1	(Adhikari & Panda, 2018)
	Saya khawatir data pribadi saya pada aplikasi Mobile JKN dapat diakses oleh pihak yang tidak berwenang.	PC2	
Kepercayaan (<i>Trust</i>)	Saya percaya aplikasi Mobile JKN aman untuk digunakan.	TR1	(Mcknight et al., 2002)
	Saya percaya BPJS menjaga keamanan data pengguna aplikasi Mobile JKN.	TR2	
	Saya percaya aplikasi Mobile JKN memiliki kemampuan teknis yang baik dan dapat digunakan dengan andal.	TR3	
Niat perilaku (<i>Behavioral Intention</i>)	Saya berniat untuk terus menggunakan aplikasi Mobile JKN untuk kebutuhan layanan kesehatan saya.	BI1	(Hassani et al., 2014)
	Saya bersedia merekomendasikan aplikasi Mobile JKN kepada orang lain	BI2	(Wiastuti et al., 2022)
	Saya lebih memilih menggunakan aplikasi Mobile JKN dibandingkan menggunakan cara lain dalam mengakses layanan BPJS.	BI3	(Gan & Li, 2015)

3. HASIL DAN PEMBAHASAN

3.1. Karakteristik Responden

Karakteristik responden dalam penelitian ini digunakan untuk memberikan gambaran umum mengenai profil responden yang berpartisipasi dalam penelitian. Data karakteristik responden diperoleh dari hasil penyebaran kuesioner kepada 120 orang pengguna aplikasi Mobile JKN yang telah memenuhi kriteria penelitian. Adapun karakteristik responden yang dianalisis meliputi jenis kelamin, usia, tingkat pendidikan, pekerjaan, dan domisili responden. Berdasarkan data yang telah diperoleh, berikut disajikan hasil karakteristik responden dalam penelitian ini.

Tabel 3. Karakteristik Responden

Karakteristik	Kategori	Jumlah	Persentase
Jenis Kelamin	Laki-laki	52	24,76%
	Perempuan	158	75,24%
Usia	< 17 tahun	0	0%
	17–20 tahun	27	12,86%
	21–25 tahun	117	55,71%
	26–30 tahun	37	17,62%
	> 30 tahun	29	13,81%
Pendidikan Terakhir	SD	0	0%
	SMP	2	0,95%
	SMA/SMK	110	52,38%
	Diploma (D3)	18	8,57%
	Sarjana (S1)	75	35,71%
	Sarjana (S2/S3)	5	2,38%
	Lainnya	0	0%
Pekerjaan	Pelajar/Mahasiswa	105	50,00%
	Pegawai Negeri	10	4,76%
	Pegawai Swasta	44	20,95%
	Wiraswasta	30	14,29%
	Lainnya	21	10,00%

3.2. Hasil Analisis Deskriptif

Analisis statistik deskriptif digunakan untuk menggambarkan karakteristik distribusi data serta kecenderungan pola jawaban responden pada setiap indikator variabel penelitian. Pengujian ini dilakukan terhadap sampel final sebanyak 210 responden pengguna aplikasi Mobile JKN. Hasil analisis deskriptif secara ringkas disajikan pada Tabel berikut:

Tabel 4. Hasil Analisis Deskriptif

Variabel	Kode	N	Persentase Jawaban				Mean	Standar Deviasi
			STS	TS	S	SS		
			(%)	(%)	(%)	(%)		
Perceived	PS1	210	0,95	2,86	36,19	60	3,552	7,133
	PS2		0,95	2,86	33,33	62,86	3,581	
Perceived vulnerability	PV1	210	5,24	12,38	54,76	27,62	3,048	0,779
	PV2		6,67	16,67	52,38	24,29	2,943	0,820
	PV3		5,71	15,71	44,29	34,29	3,071	0,851
Response efficacy	RE1	210	0,48	6,19	35,24	58,10	3,510	0,634
	RE2		1,43	7,14	41,43	50	3,400	0,685
	RE3		0,48	8,10	36,19	55,24	3,462	0,663
Self Efficacy	SE1	210	1,90	10,00	57,62	30,48	3,167	0,673
	SE2		0,48	5,24	50,48	43,81	3,376	0,607
	SE3		1,43	9,05	50,95	38,57	3,267	0,680

Variabel	Kode	N	Persentase Jawaban				Mean	$\sum$ Mean	Standar Deviasi
			STS	TS	S	SS			
			(%)	(%)	(%)	(%)			
Respon se cost	RC1	210	10,00	14,29	45,24	30,48	2,962	5,772	0,920
	RC2		12,86	18,57	43,33	25,24	2,810		0,957
Privacy concern	PC1	210	5,24	11,90	37,62	45,24	3,229	6,424	0,854
	PC2		5,71	11,90	39,52	42,86	3,195		0,859
Trust	TR1	210	1,90	15,24	51,90	30,95	3,119	9,424	0,724
	TR2		2,38	12,38	52,38	32,86	3,157		0,723
	TR3		2,38	11,43	55,24	30,95	3,148		0,705
Behavioral intention	BI1	210	0,95	6,19	53,33	39,52	3,314	9,776	0,630
	BI2		0,95	10,95	56,19	31,90	3,190		0,656
	BI3		2,38	7,14	52,38	38,10	3,262		0,692

3.3. Hasil Uji Model Pengukuran (Outer Model)

Tahap ini dilakukan untuk memastikan bahwa setiap indikator kuesioner benar-benar valid dan reliabel dalam mengukur variabelnya masing-masing. Evaluasi outer model ini dinilai berdasarkan tiga kriteria utama, yaitu validitas konvergen (*convergent validity*), validitas diskriminan (*discriminant validity*), serta uji reliabilitas.

3.3.1. Validitas Konvergen

Pengujian validitas konvergen dilakukan untuk memastikan bahwa setiap indikator mampu mengukur konstruk yang dituju secara tepat. Evaluasi validitas konvergen dilakukan dengan melihat nilai *loading factor* > 0,7 dan *Average Variance Extracted (AVE)* > 0,5 [18]. Adapun hasil pengujian validitas konvergen dalam penelitian ini disajikan pada tabel berikut.

Tabel 5. Validitas Konvergen

Variabel	Indikator	Outer Loading	AVE	Keterangan
<i>Behavioral intention</i> (BI)	BI1	0,846	0,720	Valid
	BI2	0,872		
	BI3	0,827		
<i>Privacy Concern</i> (PC)	PC1	0,956	0,869	Valid
	PC2	0,908		
<i>Perceived severity</i> (PS)	PS1	0,862	0,793	Valid
	PS2	0,918		
<i>Perceived vulnerability</i> (PV)	PV1	0,810	0,731	Valid
	PV2	0,896		
	PV3	0,856		
<i>Response Cost</i> (RC)	RC1	0,886	0,817	Valid
	RC2	0,921		
<i>Response Efficacy</i> (RE)	RE1	0,827	0,706	Valid
	RE2	0,862		
	RE3	0,832		
<i>Self efficacy</i> (SE)	SE1	0,861	0,658	Valid
	SE2	0,774		
	SE3	0,798		

Variabel	Indikator	Outer Loading	AVE	Keterangan
Trust (TR)	TR1	0,885	0,770	Valid
	TR2	0,897		
	TR3	0,850		

3.3.2. Validitas Diskriminan

Pengujian validitas diskriminan dalam penelitian ini dilakukan menggunakan *Cross Loading*. Pada pengujian *Cross Loading*, validitas diskriminan terpenuhi apabila nilai loading suatu indikator pada konstruk yang diukurnya lebih tinggi dibandingkan nilai loading pada konstruk lainnya. Hasil pengujian validitas diskriminan menunjukkan bahwa seluruh indikator telah memenuhi kriteria *cross loading* yang dipersyaratkan, disajikan pada tabel di bawah ini:

Tabel 6. Validitas Diskriminan

	BI	PC	PS	PV	RC	RE	SE	TR
BI1	0.846	-0.147	-0.111	-0.256	0.018	0.175	0.230	0.542
BI2	0.872	-0.242	-0.072	-0.309	0.189	0.251	0.358	0.611
BI3	0.827	-0.173	-0.069	-0.223	0.064	0.122	0.257	0.528
PC1	-0.239	0.956	0.232	0.505	-0.260	-0.033	-0.110	-0.351
PC2	-0.167	0.908	0.200	0.491	-0.116	-0.029	-0.089	-0.303
PS1	-0.076	0.226	0.862	0.309	0.001	0.132	0.039	-0.157
PS2	-0.097	0.196	0.918	0.357	0.032	0.070	0.025	-0.222
PV1	-0.169	0.424	0.307	0.810	-0.118	-0.102	-0.041	-0.247
PV2	-0.345	0.474	0.319	0.896	-0.068	-0.107	-0.108	-0.365
PV3	-0.231	0.469	0.347	0.856	-0.150	-0.124	-0.089	-0.250
RC1	0.092	-0.157	0.030	-0.161	0.886	0.169	0.372	0.107
RC2	0.110	-0.225	0.009	-0.067	0.921	0.242	0.357	0.094
RE1	0.163	0.050	0.105	-0.061	0.080	0.827	0.398	0.104
RE2	0.195	-0.068	0.083	-0.163	0.244	0.862	0.443	0.227
RE3	0.192	-0.054	0.089	-0.092	0.240	0.832	0.416	0.167
SE1	0.297	-0.062	0.039	-0.091	0.312	0.447	0.861	0.358
SE2	0.266	-0.088	0.079	-0.086	0.320	0.466	0.774	0.214
SE3	0.253	-0.118	-0.037	-0.065	0.351	0.295	0.798	0.331
TR1	0.569	-0.354	-0.205	-0.306	0.130	0.136	0.303	0.885
TR2	0.578	-0.319	-0.162	-0.325	0.098	0.180	0.330	0.897
TR3	0.597	-0.260	-0.202	-0.291	0.065	0.213	0.347	0.850

3.3.3. Uji Reabilitas

Uji reliabilitas merupakan pengujian yang dilakukan untuk menilai tingkat konsistensi suatu instrumen penelitian dalam mengukur variabel atau konstruk. Secara umum, instrumen dinyatakan reliabel apabila memiliki nilai *Composite Reliability* dan *Cronbach's Alpha* lebih besar dari 0,70 [19].

Tabel 7. Hasil Uji Reabilitas

Variabel	Cronbach's Alpha	Composite Reliability	Keterangan
<i>Behavioral intention</i>	0,806	0,885	Valid dan Reliabel
<i>Privacy Concern (PC)</i>	0,853	0,930	Valid dan Reliabel

Variabel	Cronbach's Alpha	Composite Reliability	Keterangan
<i>Perceived severity</i> (PS)	0,743	0,884	Valid dan Reliabel
<i>Perceived vulnerability</i> (PV)	0,826	0,890	Valid dan Reliabel
<i>Response Cost</i> (RC)	0,777	0,899	Valid dan Reliabel
<i>Response Efficacy</i> (RE)	0,793	0,878	Valid dan Reliabel
<i>Self efficacy</i> (SE)	0,740	0,852	Valid dan Reliabel
<i>Trust</i> (TR)	0,851	0,909	Valid dan Reliabel

Berdasarkan data pada Tabel 7, nilai Composite Reliability maupun Cronbach's Alpha pada semua konstruk menunjukkan angka di atas 0,70. Maka dapat disimpulkan bahwa semua konstruk memiliki reliabilitas yang baik.

3.4 Hasil Uji Model Struktural (*Inner Model*)

Tahap kedua dari analisis menggunakan PLS-SEM yaitu uji model struktural (*inner model*). Menurut [19] evaluasi model struktural (*inner model*) pada PLS-SEM dilakukan dengan menganalisis *R-Square F-Square*, *Q-Square*.

3.4.1. *R-Square*

Koefisien determinasi (R^2) digunakan untuk mengetahui seberapa besar kemampuan variabel independen dalam menjelaskan variabel dependen pada model penelitian. Nilai R^2 sebesar 0,75 menunjukkan kategori kuat (*substantial*), nilai 0,50 menunjukkan kategori sedang (*moderate*), dan nilai 0,25 menunjukkan kategori lemah (*weak*) [15].

Tabel 8. *R-Square*

Variabel	<i>R-Square</i>	Keterangan
<i>Behavioral intention</i>	0,465	Lemah

Berdasarkan Tabel 8, nilai *R-Square* (R^2) untuk variabel *Behavioral intention* sebesar 0,465. Nilai tersebut menunjukkan bahwa sebesar 46,5% variasi *Behavioral intention* dapat dijelaskan oleh variabel-variabel yang digunakan dalam penelitian ini, sedangkan 53,5% sisanya dipengaruhi oleh variabel lain yang tidak diteliti. Dengan demikian, model penelitian memiliki tingkat kemampuan penjelasan yang tergolong “lemah” (*weak*).

3.4.2. *F-Square*

Nilai f^2 menggambarkan besarnya perubahan pada nilai R^2 ketika suatu konstruk eksogen dikeluarkan dari model penelitian. Menurut Cohen (1988), nilai f^2 sebesar 0,02 dikategorikan sebagai pengaruh kecil (*small effect*), 0,15 sebagai pengaruh sedang (*medium effect*), dan 0,35 sebagai pengaruh besar (*large effect*) [21].

Tabel 8. *F-Square*

	<i>F-Square</i>	Keterangan
<i>Privacy Concern</i> -> <i>Behavioral intention</i>	0.005	Tidak Berpengaruh
<i>Perceived severity</i> -> <i>Behavioral intention</i>	0.007	Tidak Berpengaruh
<i>Perceived vulnerability</i> -> <i>Behavioral intention</i>	0.024	Kecil
<i>Response Cost</i> -> <i>Behavioral intention</i>	0.000	Tidak Berpengaruh
<i>Response Efficacy</i> -> <i>Behavioral intention</i>	0.001	Tidak Berpengaruh
<i>Self efficacy</i> -> <i>Behavioral intention</i>	0.008	Tidak Berpengaruh

	F-Square	Keterangan
<i>Trust -> Behavioral intention</i>	0,497	Besar

Berdasarkan Tabel 8, hasil pengujian F-Square (f^2) menunjukkan bahwa variabel *Trust* memiliki kontribusi terbesar terhadap *Behavioral intention* dengan nilai sebesar 0,497 yang termasuk dalam kategori besar (*large effect*). Sementara itu, variabel *Perceived vulnerability* memiliki nilai f^2 sebesar 0,024 yang termasuk dalam kategori kecil (*small effect*), dan variabel lainnya tidak berpengaruh.

3.4.1. Q-Square

Nilai Q-Square diperoleh melalui prosedur blindfolding pada SmartPLS. Model dikatakan memiliki kemampuan prediksi yang baik apabila nilai Q^2 lebih besar dari nol ($Q^2 > 0$) [15].

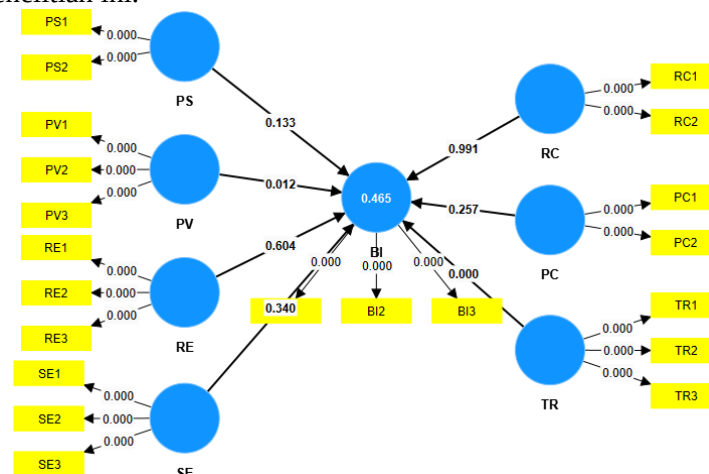
Tabel 9. Q-Square

Variabel	Q-Square	Predictive Relevance
<i>Behavioral intention</i>	0,307	Ya

Berdasarkan hasil pengolahan data pada Tabel 24, menunjukkan bahwa variabel *Behavioral intention* memiliki nilai Q-Square lebih besar dari nol, yaitu sebesar 0,307. Dengan demikian, dapat disimpulkan bahwa model penelitian memiliki *predictive relevance*.

3.4 Hasil Pengujian Hipotesis

Pengujian hipotesis dalam penelitian ini dilakukan menggunakan metode Partial Least Square Structural Equation Modeling (PLS-SEM) dengan bootstrapping pada aplikasi SmartPLS. Pengujian hipotesis bertujuan untuk mengetahui pengaruh antarvariabel dalam model penelitian. Hipotesis dinyatakan diterima apabila nilai t-statistics lebih besar dari 1,96 dan nilai p-values lebih kecil dari 0,05 pada tingkat signifikansi 5%. Sebaliknya, apabila nilai t-statistics lebih kecil dari 1,96 dan nilai p-values lebih besar dari 0,05, maka hipotesis dinyatakan ditolak. Tabel dan gambar ini memberi suatu petunjuk hasil uji hipotesis penelitian ini.



Gambar 2. Hasil Pengujian Hipotesis

Tabel 10. Hasil Pengujian Hipotesis

Hipotesis	Path Coefficient	T-Statistic	P-Values	Keterangan
H1: PS -> BI	0,068	1,504	0,133	Ditolak
H2: PV -> BI	-0,146	2,520	0,012	Diterima
H3: RE -> BI	0,031	0,519	0,604	Ditolak
H4: SE -> BI	0,083	0,953	0,340	Ditolak
H5: RC -> BI	-0,001	0,011	0,991	Ditolak

Hipotesis	Path Coefficient	T-Statistic	P-Values	Keterangan
H6: PC -> BI	0,064	1,133	0,257	Ditolak
H7: TR -> BI	0,612	8,976	0,000	Diterima

Berdasarkan Tabel 10, didapatkan hasil sebagai berikut:

1. **H1 ditolak.** *Perceived severity* (PS) mempunyai pengaruh positif namun tidak signifikan terhadap *Behavioral intention* (BI), dengan nilai path coefficient sebesar 0,068, t-statistic sebesar 1,504 ($< 1,96$), serta p-values sebesar 0,133 ($> 0,05$). Hal ini menunjukkan bahwa persepsi pengguna terhadap tingkat keparahan dampak kebocoran data belum mampu memengaruhi niat penggunaan aplikasi Mobile JKN secara signifikan.
2. **H2 diterima.** *Perceived vulnerability* (PV) berpengaruh negatif dan signifikan terhadap *Behavioral intention* (BI), dengan nilai path coefficient sebesar -0,146, t-statistic sebesar 2,520 ($> 1,96$), serta p-values sebesar 0,012 ($< 0,05$). Artinya, semakin tinggi persepsi pengguna terhadap kerentanan data pribadinya, semakin menurun niat penggunaan aplikasi Mobile JKN. Hal ini mengindikasikan bahwa kekhawatiran akan kerentanan data justru mendorong pengguna untuk menahan diri atau berhati-hati dalam menggunakan aplikasi.
3. **H3 ditolak.** *Response Efficacy* (RE) mempunyai pengaruh positif namun tidak signifikan terhadap *Behavioral intention* (BI), dengan nilai path coefficient sebesar 0,031, t-statistic sebesar 0,519 ($< 1,96$), serta p-values sebesar 0,604 ($> 0,05$). Hal ini mengindikasikan bahwa keyakinan pengguna terhadap efektivitas mekanisme keamanan aplikasi belum menjadi faktor utama dalam meningkatkan niat penggunaan.
4. **H4 ditolak.** *Self-Efficacy* (SE) mempunyai pengaruh positif namun tidak signifikan terhadap *Behavioral intention* (BI), dengan nilai path coefficient sebesar 0,083, t-statistic sebesar 0,953 ($< 1,96$), serta p-values sebesar 0,340 ($> 0,05$). Hal ini menunjukkan bahwa keyakinan pengguna terhadap kemampuan dirinya sendiri dalam menjaga keamanan data belum berpengaruh signifikan terhadap niat penggunaan aplikasi.
5. **H5 ditolak.** *Response Cost* (RC) mempunyai pengaruh negatif namun tidak signifikan terhadap *Behavioral intention* (BI), dengan nilai path coefficient sebesar -0,001, t-statistic sebesar 0,011 ($< 1,96$), serta p-values sebesar 0,991 ($> 0,05$). Artinya, persepsi mengenai biaya atau usaha untuk menerapkan tindakan keamanan hampir tidak memberikan pengaruh apa pun terhadap niat pengguna.
6. **H6 ditolak.** *Privacy Concern* (PC) mempunyai pengaruh positif namun tidak signifikan terhadap *Behavioral intention* (BI), dengan nilai path coefficient sebesar 0,064, t-statistic sebesar 1,133 ($< 1,96$), serta p-values sebesar 0,257 ($> 0,05$). Hal ini menunjukkan bahwa kekhawatiran pengguna terhadap privasi data belum berpengaruh signifikan terhadap niat penggunaan aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan.
7. **H7 diterima.** *Trust* (TR) berpengaruh positif dan signifikan terhadap *Behavioral intention* (BI), dengan nilai path coefficient sebesar 0,612, t-statistic sebesar 8,976 ($> 1,96$), serta p-values sebesar 0,000 ($< 0,05$). Artinya, semakin tinggi kepercayaan pengguna terhadap kemampuan Mobile JKN dan BPJS Kesehatan dalam mengelola serta melindungi data pribadi, semakin tinggi pula niat penggunaan aplikasi tersebut. *Trust* menjadi faktor paling dominan dalam memengaruhi niat penggunaan pada model penelitian ini.

3.5. Pembahasan

Adapun pembahasan secara detail berdasarkan tabel 10 hasil pengujian hipotesis yang diuraikan adalah sebagai berikut:

H1: *Perceived severity* berpengaruh negatif terhadap *Behavioral intention* — Ditolak

Perceived severity tidak berpengaruh signifikan terhadap *Behavioral intention*. Pengguna menyadari risiko kebocoran data, namun manfaat dan kemudahan layanan Mobile JKN dianggap lebih penting sehingga risiko tersebut tidak menjadi pertimbangan utama.

H2: *Perceived vulnerability* berpengaruh negatif terhadap *Behavioral intention* — Diterima

Perceived vulnerability berpengaruh negatif signifikan (pengaruh kecil). Semakin tinggi persepsi kerentanan pengguna terhadap penyalahgunaan data, semakin rendah niat penggunaan, sejalan dengan asumsi PMT bahwa kerentanan yang dirasakan mendorong sikap menghindar.

H3: Response Efficacy berpengaruh positif terhadap Behavioral intention — Ditolak

Response efficacy tidak berpengaruh signifikan. Mekanisme perlindungan data Mobile JKN bersifat administratif/backend (enkripsi, audit sistem) sehingga efektivitasnya kurang dirasakan langsung oleh pengguna awam.

H4: Self Efficacy berpengaruh positif terhadap Behavioral intention — Ditolak

Self-efficacy tidak berpengaruh signifikan. Pengguna tetap menggunakan aplikasi karena kebutuhan layanan, bukan karena kemampuan pribadi dalam menjaga keamanan data, yang dianggap sudah lazim dimiliki pengguna aplikasi digital.

H5: Response Cost berpengaruh negatif terhadap Behavioral intention — Ditolak

Response cost tidak berpengaruh signifikan. Upaya atau pengorbanan dalam menjaga keamanan data tidak dirasakan sebagai beban, karena pengguna telah terbiasa dengan proses verifikasi dan pengamanan akun pada aplikasi digital lain.

H6: Privacy Concern berpengaruh negatif terhadap Behavioral intention — Ditolak

Privacy concern tidak berpengaruh signifikan. Kekhawatiran privasi tidak cukup kuat mengubah niat penggunaan karena Mobile JKN memiliki manfaat penting dan sulit digantikan.

H7: Trust berpengaruh positif terhadap Behavioral intention — Diterima

Trust berpengaruh positif signifikan dengan pengaruh besar, jauh melampaui variabel lain. Kepercayaan terhadap keamanan sistem, perlindungan data, dan keandalan layanan membuat pengguna tetap menggunakan Mobile JKN meski pernah terjadi kebocoran data. Data kuesioner pendukung menunjukkan mayoritas responden bertahan karena percaya BPJS telah memperbaiki sistem keamanan dan karena kebutuhan esensial berobat, menegaskan dominasi *trust* dan indikasi *privacy paradox*.

Dari tujuh hipotesis, hanya H2 (*perceived vulnerability*) dan H7 (*trust*) yang signifikan, dengan *trust* sebagai faktor paling dominan. Niat penggunaan Mobile JKN lebih ditentukan oleh kepercayaan terhadap penyedia layanan dan sifat layanan kesehatan publik yang esensial, dibandingkan evaluasi ancaman atau coping secara kognitif.

4. KESIMPULAN

Temuan penelitian ini mengonfirmasi bahwa dari tujuh variabel yang diuji dalam kerangka *Protection Motivation Theory* (PMT), *Perceived vulnerability* dan *Trust* merupakan faktor yang secara nyata membentuk *Behavioral intention* pengguna aplikasi Mobile JKN pascakebocoran data BPJS Kesehatan. *Trust* tampil sebagai penentu paling kuat dalam model, sementara *Perceived vulnerability* memberikan pengaruh ke arah sebaliknya (negatif), yang berarti semakin pengguna merasa data pribadinya rentan disalahgunakan, semakin besar pula kecenderungan mereka untuk mengurangi niat penggunaan aplikasi. Dengan kata lain, keberlanjutan penggunaan Mobile JKN pascainsiden kebocoran data lebih banyak ditopang oleh seberapa besar kepercayaan pengguna terhadap sistem, dibandingkan oleh seberapa besar rasa takut atau ancaman yang mereka rasakan.

Sementara itu, kelima variabel lainnya—*Perceived Severity*, *Response Efficacy*, *Self-Efficacy*, *Response Cost*, dan *Privacy Concern*—belum terbukti berpengaruh secara signifikan terhadap niat pengguna untuk tetap memakai aplikasi. Kondisi ini mengisyaratkan bahwa persepsi keparahan dampak kebocoran data, keyakinan atas efektivitas langkah pengamanan, kemampuan diri dalam menjaga keamanan akun, beban usaha yang harus dikeluarkan, hingga kekhawatiran privasi itu sendiri, belum cukup kuat untuk mengubah keputusan pengguna dalam konteks layanan kesehatan digital yang bersifat publik dan minim alternatif seperti Mobile JKN.

Guna memperdalam pemahaman atas fenomena ini, penelitian berikutnya perlu mempertimbangkan penambahan variabel lain yang berpotensi relevan, seperti ketergantungan pengguna terhadap layanan (*service dependency*) atau kualitas layanan aplikasi, sekaligus memperbesar jumlah dan sebaran responden agar hasil lebih representatif secara nasional. Selain itu, penelitian selanjutnya juga disarankan menelusuri kemungkinan peran *Trust* sebagai variabel mediasi antara *Privacy Concern* dan *Behavioral intention*, mengingat pola hubungan di antara kedua variabel tersebut cukup menonjol dalam hasil analisis penelitian ini.

Daftar Pustaka

- [1] Febrianti, Z. S., & Devega, M. Analisis Sentimen Terhadap Penggunaan Aplikasi Mobile Jkn Dengan Pendekatan Random Forest Classifier, ZONAsi, 2025, 7(3), 1081–1091.
- [2] Ginting, R., Asdar, J., Samura, P., Parinduri, A. I., Br, S. M., & Hasanah, D. N. Hubungan Pemanfaatan Aplikasi Mobile Jaminan Kesehatan Nasional (JKN) dengan Pelayanan Kesehatan, JKf, 2024; c, 97–101.
- [3] Nugraha, D. A., Nurfitroh, R., Ul-Haq, N. D., Dika, R. P., & Lagontang, S. N.. Kebocoran Data Bpjs Kesehatan: Ancaman Terhadap Keamanan Informasi Publik Di Era Digital, IPSSJ, 2021, 2(3), 4685–4691.
- [4] Munandar, A., Listiani, D., Malik, F. A., Pratama, B. A., & Elfina, A. Kebocoran Data BPJS sebagai Studi Kasus Kelemahan Keamanan Lembaga Publik, TEKNOBIS, 2025, 3(2), 2023–2026.
- [5] Sorisa, C., & Kiareni, C. L. Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia Cinda. Jurnal Sains Student Research, 2024, Vol.2, 2(6), 586–593.
- [6] Kusumawati, R. M., Wulandari, K., Masyarakat, K., Masyarakat, F. K., Widya, U., Mahakam, G., Wahid, J., & No, H. JKN Mobile Application Utilization. Jurnal Kebijakan Kesehatan Indonesia (JKKI), 2024, 13(01), 52–55.
- [7] Meier, Y., & Krämer, N. C. *A longitudinal examination of Internet users ' privacy protection behaviors in relation to their perceived collective value of privacy and individual privacy concerns*, Article reuse guidelines, 2024, Vol. 26(10) 5942 –5961
- [8] Setiawan, F. S. Analisis kepercayaan pengguna TikTok terhadap sistem rekomendasi tiktok yang berbasis *Artificial Intelligence* (AI) dengan model Trust In AI, Academia.Edu, 2024, 240160121134.
- [9] D., M., & S., P. *Protection Motivation Theory: A review*. In S. Papagiannidis (Ed), TheoryHub Book, 2025.
- [10] Rogers W., R. *Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation*. *Social Psychophysiology: A Sourcebook*, January 1983, 153–177.
- [11] Syafiqah, F., Pinandito, A., & Rokhmawati, R. I. Analisis Kesediaan User Permission pada Fitur App Tracking Transparency melalui pendekatan *Protection Motivation Theory*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Januari 2017, 1(1), 1–9.
- [12] Putri, D. Y., Suratno, T., & Noverina, Y. Kesadaran Privasi Data Dan Kepercayaan Pengguna Aplikasi Seabank Menggunakan Protection Motivation Theory. Jati, 2025, 9(4), 6207–6214.
- [13] Rogers W., R. *Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation*. *Social Psychophysiology: A Sourcebook*, January 1983, 153–177.
- [14] Untari, D. T. Metodologi Penelitian. In Pena Persada, Banyumas, Jawa Tengah, Indonesia. CV. Perna Persada, 2018
- [15] Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. A Primer on partial least squares Structural Equation Modeling (PLS-SEM). In European Journal of Tourism Research, 2022, (Vol. 6, Issue 2, pp. 211–213).
- [16] Workman, M., Bommer, W. H., & Straub, D.. Computers in Human Behavior Security lapses and the omission of information security measures: A threat control model and empirical test, 2008 24, 2799–2816.
- [17] Vance, A., Siponen, M., & Pahnla, S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Elsevier, 2012 49, 190–192.
- [18] Yarsasi, S., Tahyudin, I., & Hariguna, T. Analisis Validitas dan Reliabilitas Kuesioner dengan Metode Partial Least Squares Structural Equation Modeling pada Aplikasi SMARTPLS Analysis of Validity and Reliability of Questionnaires Using Partial Least Squares Structural Equation Modeling Method on. 2025, 5(7), 1905–1913.
- [19] Sanaky, M. M., Saleh, L. M., & Titaley, D. H. Uji Reabilitas. Jurnal Simetrik, 2021, 11(1), 432–439.

- [20] Hair, J. F., Hult, G. T., Ringle, C., & Sarstedt, M. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) - Joseph F. Hair, Jr., G. Tomas M. Hult, Christian Ringle, Marko Sarstedt. In Sage, 2017
- [21] Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. Partial Least



ZONAsi: Jurnal Sistem Informasi

Is licensed under a [Creative Commons Attribution International \(CC BY-SA 4.0\)](https://creativecommons.org/licenses/by-sa/4.0/)