Jurnal PETISI, Vol. 07, No. 02, April 2026
e-ISSN: 2721-6276

Pengaruh Kesadaran Privasi Data Terhadap Perilaku Pemain Gacha Games Online

Muhammad Arif Firdaus[1], Tri Suratno[2], Yolla Noverina[3]
Universitas Jambi
arffqh231103@gmail.com[1], tri@unja.ac.id[2], yollanoverina@unja.ac.id[3].

Abstrak: Game gacha merupakan pendekatan penjualan khusus, di mana penjual menjual gacha pull kepada pembeli, saat ini terdapat dua judul game yang sedang populer dimainkan yaitu Genshin Impact dan Wuthering Waves. Namun, di balik kesuksesannya, muncul berbagai masalah, salah satu yang menjadi permasalahan dalam perkembangan game-game ini adalah permasalahan terkait privasi data. Menggunakan *Security Belief Model* yang mana dapat memberikan kerangka kerja yang kuat dalam memahami perilaku pengguna online terkait Privasi data dan keamanan Privasi data. Hasil PLS-SEM menunjukkan *Security Awareness* (SA) signifikan mempengaruhi *Self-Efficacy in Information Security(*SEIS*)* dan *Perceived Security Threat* (PT). Kesadaran akan bahaya mendorong pemain lebih percaya diri dan waspada. SEIS signifikan mempengaruhi Expectations (EPB). *Perceived Security Threat* (PT) signifikan mempengaruhi *Concern for Information Privacy* (CIP) dan *Security Behavior* (SB). Expectations juga signifikan mempengaruhi SB. Meskipun CIP tidak signifikan mempengaruhi SB, SA memiliki pengaruh tidak langsung yang signifikan terhadap SB melalui variabel mediasi yang ada. Ini menunjukkan kesadaran yang tinggi menghasilkan perilaku privasi data yang lebih baik.
Kata Kunci : Sistem informasi. privasi data, s*ecurity belief model*, kesadaran privasi data, perilaku privasi data.

Abstract: *Gacha games are a specialized sales approach, where sellers sell gacha pulls to buyers. Currently, two popular game titles are Genshin Impact and Wuthering Waves. However, behind their success, various issues arise, one of which is the issue related to data privacy. Using the Security Belief Model, which can provide a strong framework in understanding online user behavior related to data privacy and data security. PLS-SEM results show that Security Awareness (SA) significantly influences Self-Efficacy in Information Security (SEIS) and Perceived Security Threat (PT). Awareness of danger makes players more confident and alert. SEIS significantly influences Expectations (EPB). Perceived Security Threat (PT) significantly influences Concern for Information Privacy (CIP) and Security Behavior (SB). Expectations also significantly influence SB. Although CIP does not significantly influence SB, SA has a significant indirect effect on SB through existing mediating variables. This indicates that high awareness results in better data privacy behavior.*
***Keyword**s: information Systems, Data Privacy, Security Belief Model, Security Awareness, Security Behavior*

1. Pendahuluan

Game gacha merupakan pendekatan penjualan khusus, di mana penjual menjual gacha pull kepada pembeli. Setiap gacha pull akan memberikan kemungkinan tertentu bagi pembeli agar dapat memenangkan hadiah yang ada di dalam game gacha tersebut(Toto, 2021)Game gacha telah digunakan secara antusias dalam berbagai video game online dan

memiliki berbagai macam potensi dalam pengembangan aplikasi yang menggunakan model ini. Salah satu aplikasi game gacha yang paling populer adalah model gacha yang diaplikasikan dalam video game(Chen & Fang, 2023). Namun, di balik kesuksesannya, muncul berbagai masalah, salah satu yang menjadi permasalahan dalam perkembangan game-game ini adalah permasalahan terkait privasi data. Masalah terkait Privasi data ini bisa saja berasal dari luar game tersebut seperti Tindakan Scam atau Phising melalui platform media sosial atau bahkan berasal dari dalam game tersebut seperti melalui Fitur Chat dari dalam game(aisisoda, 2024; BetaNebula, 2023; Muhammad Naufal, 2024).

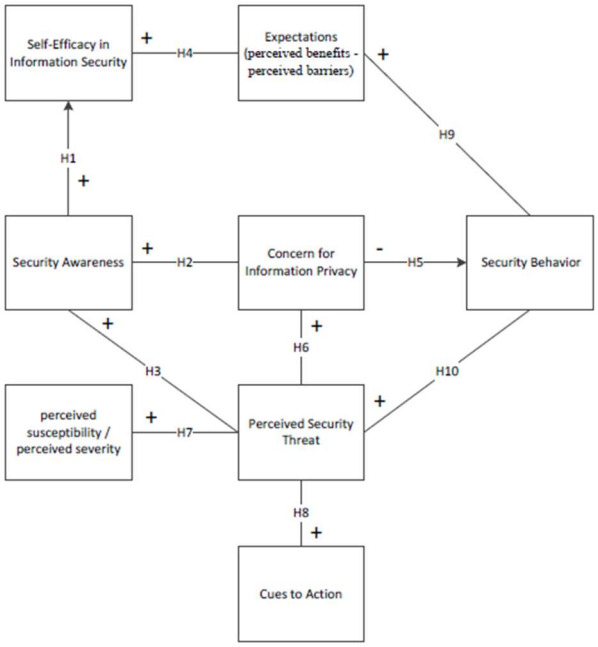
Tingkat kesadaran pemain terhadap pentingnya menjaga Privasi Data pribadinya pada saat bermain game tersebut menjadi salah satu faktor yang harus dikuasai oleh setiap pemain dan juga tentunya oleh setiap kalangan masyarakat. Kesadaran keamanan informasi bisa didefinisikan bahwa seseorang memiliki pengetahuan atau kemampuan yang baik dalam melakukan praktik keamanan pada saat menggunakan situs jejaring internet dan memahami arti penting melindungi data pribadi dan atau data kelompok atas nama sebuah organisasi ketika memutuskan akan menggunakan sebuah situs jejaring internet(Edwards, 2015). Kesadaran privasi adalah pemahaman tentang hak individu untuk mengontrol informasi pribadi miliknya dan mengontrol arus berjalannya informasi yang berisikan data tentang dirinya menyebar. Ini mencakup kesadaran akan pentingnya melindungi data pribadi dari akses, penggunaan, atau pengungkapan yang tidak sah. Kesadaran privasi juga melibatkan pemahaman tentang risiko yang terkait dengan pengungkapan informasi pribadi dan kemampuan untuk mengambil langkah-langkah yang diperlukan untuk melindungi privasi(Permana & Rakhmawati, 2023).

Selain dari peningkatan Kesadaran privasi data, Perilaku pemain juga harus dapat sejalan dengan pemaham mereka terkait resiko yang ada dan ancaman yang dapat memberikan dampak kepada pemain, Hal ini dikarenakan, Meskipun seorang individu memiliki pengetahuan yang baik akan keamanan dan privasi datanya, nyatanya perilaku mereka dalam melindungi data pribadi sering kali tidak sejalan dengan pengetahuan tersebut(Bada et al., 2019; Zahwani1 et al., 2023). *Security Behavior* didefinisikan sebagai perilaku atau aktivitas dalam melindungi data kepemilikan baik privasi atau data dari suatu Kelompok organisasi pada saat menggunakan atau menjelajah jaringan internet (Edwards, 2015). Perilaku Keamanan (*Security Behaviour*) dapat dipengaruhi oleh Kesadaran Keamanan privasi data, dimana dengan tingkat kesadaran privasi data ini biasanya akan memberikan pemahaman akan pentingnya mengambil tindakan dalam melindungi data baik itu individu ataupun kelompok. Tentunya kesadaran saja tidak akan membuat suatu individu mengambil tindakan secara langsung terhadap keamanan datanya, Dengan kesadaran akan menjaga privasi datanya, seorang individu atau kelompok dapat mengetahui tentang Kekhawatiran terhadap Privasi datanya, Persepsi terhadap Ancaman, dan ekspektasi yang akan didapat apabila menerapkan tindakan keamanan dalam melindungi datanya. Dengan tingkat kesadaran yang tinggi ini pengguna juga perlu mendapat motivasi dan memiliki kemampuan yang baik dalam mengambil tindakan keamanan privasi datanya (Bada et al., 2019; Fathni et al., n.d.).

Penelitian mengenai kesadaran dan perilaku privasi data dalam konteks game gacha seperti Genshin Impact dan Wuthering Waves memiliki relevansi yang sangat tinggi di era digital saat ini. dengan semakin populernya game online, terutama game gacha, penting untuk memahami bagaimana kesadaran privasi data berkembang dalam konteks yang berbeda. Penelitian ini bertujuan untuk mengisi kesenjangan ini dengan fokus pada game

gacha. Seiring dengan meningkatnya popularitas game online dan semakin kompleksnya interaksi digital, isu terkait privasi data menjadi hal yang semakin krusial. Pemahaman yang mendalam dari seorang pemain game dalam memahami dan merespons isu privasi data akan memberikan kontribusi penting dalam pengembangan kebijakan perlindungan data yang lebih efektif dan relevan dengan kebutuhan generasi muda (Chen & Fang, 2023; Dewi & Natalia, 2021; Haulussy, 2024; Jacked Yuan, 2025; Pertiwi et al., n.d.).

Security Belief Model digunakan dalam penelitian sebagai model penelitian, Security Belief Model merupakan model penelitian yang merupakan pengembangan dari model penelitian Health Belief Model sebagaimana yang dapat dilihat pada **Gambar 1**, Security Belief Model dapat memberikan kerangka kerja yang kuat dalam memahami perilaku pengguna online terkait Privasi data dan keamanan Privasi data. Dengan berfokus pada konstruksi yang relevan langsung dengan lingkungan digital, Security Belief Model dapat memberikan peningkatan kemampuan untuk mengembangkan intervensi efektif dan program kesadaran yang disesuaikan dengan tantangan unik privasi data dalam game gacha online dan platform lainnya (Du et al., 2024; Edwards, 2015; Williams et al., 2014).



Gambar 1. Security Belief Model

Penelitian ini bertujuan untuk mengisi kekosongan pengetahuan mengenai kesadaran privasi data di kalangan pemain game gacha dengan fokus pada Genshin Impact dan Wuthering Waves. Secara spesifik, penelitian ini akan menjawab pertanyaan yang ada berdasarkan kerangka model yang dimiliki oleh *Security Belief* Model dengan 8 variabel yaitu *Security Awareness (SA), Security Behavior (SB), Self–efficacy in Information Security(SEIS), Expectations (Perceived Benefits–Perceived Barriers)(EPB), Concern for Information Privacy (CIP), Perceived Susceptibility /Perceived Severity (PS), Perceived Security Threat (PT), dan Cues to Action (CTA)*, dengan mengetahui hubungan yang dimiliki dari variabel tersebut dimulai dari *Security Awareness* (SA) yang dapat memberikan pengaruh tidak langsung pada *Security Behavior* (SB) melalui variabel

mediasi dari Security Belief Model ini, penelitian ini diharapkan dapat memberikan kontribusi penting dalam pengembangan strategi untuk meningkatkan perlindungan data pribadi dalam industri game. Selain itu, penelitian ini juga diharapkan dapat memberikan pemahaman yang lebih mendalam tentang dinamika privasi data dalam konteks hiburan digital yang terus berkembang.

2. Metode Penelitian

Penelitian ini merupakan penelitian Kuantitatif dengan responden yang masuk kedalam penelitian ini adalah pemain dari game Genshin Impact dan Wuthering Waves Indonesia yang dimana total populasi sampel diambil dari total anggota grup Facebook resmi dari kedua game tersebut pada tanggal 13 Mei 2025 dengan total Pemain Genhsin Impact adalah sebesar 351,3 ribu pemain dan Wuthering Waves sebesar 108,1 ribu pemain, sehingga total populasi adalah 459,4 ribu pemain. Dengan menggunakan rumus Slovin, didapatlah total minimal responden yang dibutuhkan.

Rumus Metode Slovin :

$$n = \frac{N}{1 + (Ne^2)}$$

Penjelasan Simbol:

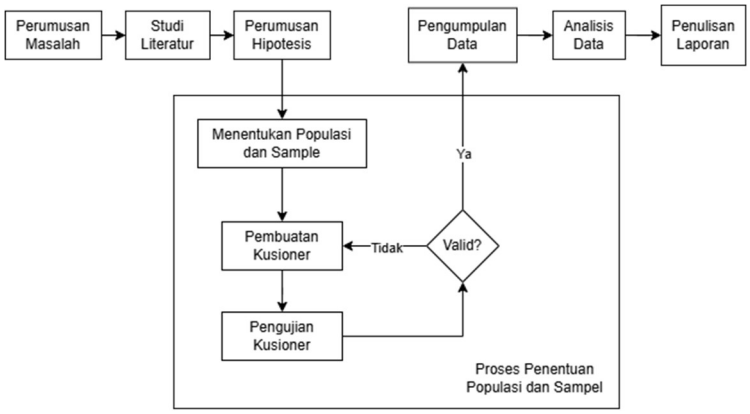
n : jumlah sampel.
N : jumlah populasi.
e : batas toleransi kesalahan (error tolerance) = 10% = 0,1.

$$n = \frac{459400}{1 + (459400(0.1^2))}$$
$$n = 99.99$$

Dari hasil Metode Slovin diatas didapatlah bahwa Jumlah responden yang akan menjadi data dalam penelitian ini adalah sebesar 99.99 orang atau dibulatkan sebanyak 100 orang.Data diperoleh dengan menggunakan Metode Kuesioner yang disebar melalui media sosial pada grup komunitas Game Gacha Online Genshin Impact dan Wuthering Waves.Adapun kriteria dari responden yang akan mengisi Kuesioner ini adalah sebagai berikut:

1.Merupakan Pemain dari game Wuthering Waves ataupun Genshin Impact;
2.Pernah melakukan Co-op pada saat bermain;
3.Pernah Menggunakan Fitur Chat di dalam game;
4.Pernah melakukan Pembelian di dalam game atau In-Game Purchase.
5.Pernah Menggunakan Layanan Joki.

Adapun langkah kerja penelitian ini sebagaimana yang dapat dilihat pada **Gambar 2** dibawah ini. Langkah kerja penelitian (Priadana & Sunarsi, 2021).



Gambar 2. Langkah Kerja Penelitian Kuantitatif

Teknik Pengumpulan data adalah langkah yang penting untuk dilakukan dalam proses penelitian, karena tujuan utama dari penelitian adalah mendapatkan data(Priadana & Sunarsi, 2021). Dalam penelitian ini pengumpulan data akan dilakukan dengan menggunakan kusioner dengan menggunakan skala likert ganjil 5 pilihan, Pemilihan penggunaan Skala likert ini didasarkan pada kemampuan dari skala likert berpilihan ganjil memiliki tingkat validitas dan reliabilitas yang lebih efektif dibandingkan dengan skala likert berpilihan genap (Borgo et al., 2022; Garland, 1991; Kusmaryono et al., 2022).

Penelitian ini akan menggunakan salah satu model dari SEM yaitu Partial Least Squares - Structural Equation Model(PLS-SEM) sebagai Teknik analisis. Penggunaan PLS-SEM sebagai Teknik analisis dikarenakan model PLS-SEM dapat memungkinkan peneliti untuk melakukan analisis dari hubungan yang dilakukan secara bersamaan di dalam suatu model yang kompleks, model tersebut dapat terdiri dari beberapa konstruksi, variable indicator, dan jalur structural (Dedi & Rianto Rahadi, 2023; Hair et al., 2022) untuk membantu dalam menemukan hasil penelitian, akan digunakan software SmartPLS 4 dalam menyelesaikan penelitian ini.

Penelitian ini juga akan melakukan pengujian Hipotesis dengan menggunakan nilai P (P value) dengan membandingkan nilai dari P value dengan tingkat signifikansi (α) sebesar 10% atau 0,1. Dimana apabila nilai P lebih kecil dari pada tingkat signifikansi (α), maka Hipotesis Diterima, sedangkan apabila nilai P lebih besar dibandingkan tingkat signifikansi (α), maka hipotesis ditolak(Dedi & Rianto Rahadi, 2023; Hair et al., 2022).

Adapun hipotesis dalam penelitian ini sebagaimana sesuai dengan model penelitian yang digunakan yaitu *Security Belief Model,* Hipotesis penelitiannya adalah sebagai berikut:

a. **H1** : Adanya hubungan antara kesadaran privasi terhadap keamanan (*security awareness*) (SA) dan pengetahuan Pemain dalam memahami praktik keamanan informasi (*self-efficacy in information security*) (SEIS).
b. **H2** : Adanya hubungan antara kesadaran privasi terhadap keamanan (*security awareness*) (SA) dan tingkat perhatian pemain terhadap informasi data yang mereka berikan ketika berinteraksi terlebih dalam praktik privasi informasi (*Concern for Information Privacy*) (CIP).

c. **H3** : Adanya hubungan antara kesadaran privasi terhadap keamanan (*security awareness*) (SA) dan persepsi Pemain terhadap ancaman keamanan (*perceived security threa*t) (PT).
d. **H4** : Adanya hubungan antara pengetahuan Pemain dalam memahami praktik keamanan informasi (*self-efficacy in information security*) (SEIS) dan harapan Pemain (*expectations perceived benefits–perceived barriers*) (EPB).
e. **H5** : Ada hubungan antara tingkat perhatian pemain terhadap informasi data yang mereka berikan ketika berinteraksi terlebih dalam praktik privasi informasi (*Concern for Information Privacy*) (CIP) dan perilaku keamanan dari pemain (*Security Behavior*) (SB).
f. **H6** : Adanya hubungan antara persepsi Pemain terhadap ancaman keamanan (*perceived security threat*) (PT) dan kewajaran Pemain dalam berinteraksi dan pada saat bermain terlebih dalam praktik privasi informasi personal informasi (*Concern for Information Privacy*) (CIP).
g. **H7** : Adanya hubungan antara persepsi kelemahan/persepsi keparahan (*perceived susceptibility/perceived severity*) (PS) dan persepsi Pemain terhadap ancaman keamanan (*perceived security threat*) (PT).
h. **H8** : Adanya hubungan antara aktivitas yang memotivasi untuk merubah perilaku Pemain (*cues to action*) (CTA) dan persepsi Pemain terhadap ancaman keamanan (*perceived security threat*) (PT).
i. **H9** : Adanya hubungan antara harapan Pemain (persepsi kemanfaatan–persepsi hambatan (*expectations perceived benefits–perceived barriers*)) (EPB) dan perilaku keamanan (*security behavior*) (SB).
j. **H10** : Adanya hubungan antara persepsi Pemain terhadap ancaman keamanan (*perceived security threat*) (PT) dan perilaku keamanan (*security behavior*) (SB).

3. Hasil dan Pembahasan

Data responden yang didapat dari penyebaran kuesioner yang dilakukan pada grup Facebook dari game Genshin Impact dan Wuthering Waves, didapatlah total 103 responden yang mengisi kuesioner dengan keterangan penyebaran pemain seperti yang dapat dilihat pada **Tabel 1** dan **Tabel 2**. Pada **Tabel 1** perbandingan responden berdasarkan jenis kelamin dengan responden yang mengisi didominasi oleh Laki-Laki, sedangkan pada **Tabel 2** dilihat penyebaran merata dari banyak nya pemain yang mengisi kuesioner penelitian.

Tabel 1. Berdasarkan Jenis Kelamin

Berdasarkan Jenis Kelamin

Jenis Kelamin	Jumlah Pemain	Presentase
Laki - laki	80	78%
Perempuan	23	22%
Total	103	100%

Tabel 2. Berdasarkan Game yang dimainkan

Berdasarkan Game yang dimainkan		
Game Yang dimainkan	Jumlah Pemain	Presentase
Genshin Impact	31	30%
Saya memainkan keduanya	39	38%
Wuthering Waves	33	32%
Total	103	100%

a. Outer Model PLS-SEM

Terdapat 3 tahapan dalam pengujian outer model dari pls-sem, yaitu pengujian validitas konvergen, validitas diskriminan dan uji reliabilitas. Untuk **Validitas Konvergen**, dilakukan dengan cara membandingkan nilai outer loading model. Yang dimana apabila nilai outer loading yang dimiliki lebih besar dari pada 0,7. Namun apabila nilai dari outer loading yang didapatkan sudah mencapai nilai yang lebih besar dari 0,6 atau 0,5 dibandingkan dengan outer loading indikator, uji validitas konvergen sudah dapat dikatakan valid (Dedi & Rianto Rahadi, 2023) Hasil dari pengujian validitas konvergen dapat dilihat pada **Tabel 3**, dimana dapat terlihat semua indikator dari variabel penelitian dapat dinyatakan valid.

Tabel 3. Hasil Uji Validitas Konvergen

Indikator	CIP	CTA	EPB	PS	PT	SA	SB	SEIS
CIP1	0.905							
CIP2	0.923							
CIP3	0.808							
CIP4	0.843							
CTA1		0.666						
CTA2		0.810						
CTA3		0.660						
CTA4		0.749						
EPB1			0.856					
EPB2			0.712					
EPB3			0.664					
EPB4			0.667					
PS1				0.534				
PS2				0.905				
PS3				0.667				
PS4				0.756				
PT1					0.759			
PT2					0.838			
PT3					0.766			
PT4					0.790			
SA1						0.616		
SA2						0.593		
SA3						0.783		
SA4						0.894		
SB1							0.898	

SB2	0.779	
SB3	0.865	
SEIS1		0.819
SEIS2		0.830
SEIS3		0.639
SEIS4		0.780

Validitas diskriminan dilakukan untuk menguji apakah tes yang dirancang untuk mengukur konstruk tertentu tidak akan berkorelasi dengan tes yang mengukur konstruk yang berbeda(Dedi & Rianto Rahadi, 2023; Hair et al., 2022). Pengujian Validitas Diskriminan dilakukan dengan menggunakan metode HTMT atau Rasio Heterotrait-Monotrait. Pengujian validitas diskriminan dengan menggunakan HTMT adalah dengan menguji apakah nilai yang didapat tidak melebihi nilai ambang pada HTMT, nilai ambang HTMT yaitu 0,9(Dedi & Rianto Rahadi, 2023). Hasil dari pengujian ini dapat dilihat pada **Tabel 4.** Dapat dilihat bahwa hasil dari pengujian validitas diskriminan dimana semua variabel memiliki nilai yang tidak melebihi ambang HTMT yaitu 0,9 dan dinyatakan lolos pengujian validitas diskriminan.

Tabel 4. Hasil Uji Validitas Diskriminan

Variabel	CIP	CTA	EPB	PS	PT	SA	SB	SEIS
CIP								
CTA	0.608							
EPB	0.452	0.748						
PS	0.549	0.758	0.541					
PT	0.390	0.363	0.182	0.300				
SA	0.271	0.528	0.335	0.226	0.403			
SB	0.274	0.510	0.296	0.512	0.506	0.370		
SEIS	0.158	0.473	0.358	0.242	0.243	0.332	0.427	

Pengujian selanjutnya yang dilakukan adalah **pengujian Reliabilitas**, Pengujian Reliabilitas dilakukan dengan cara membandingkan nilai dari Komposit reliabilitas atau Composite Reliability > 0,7. Composite Reliability akan mengukur seberapa baik variabel yang mendasari konstruksi disajikan dalam pemodelan persamaan struktural(Dedi & Rianto Rahadi, 2023). Pada **Tabel 5** dapat dilihat dimana nilai dari composite reliability(Rho_a) yang dimiliki oleh tiap variabel nya memiliki nilai yang lebih besar sama dengan 0,7. Dan untuk untuk nilai dari Cronbach's alpha dan koefisien reliabilitas(Rho_c) dari tiap variabel yang ada pada pilot test ini pun sudah memiliki nilai lebih dari 0,7. Sehingga dapat dikatakan bahwa pilot test ini telah reliabel.

Tabel 5. Hasil Uji Reliabilitas

Variabel	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)
SA	0.746	0.922	0.818
SEIS	0.772	0.795	0.853
EPB	0.754	0.867	0.818
CIP	0.895	0.926	0.926
PS	0.764	0.849	0.813
CTA	0.725	0.750	0.814
PT	0.799	0.804	0.868
SB	0.805	0.819	0.885

b. Inner Model PLS-SEM

Uji Multikolinier (Inner VIF)

Pengujian ini dilakukan untuk melihat multikolinearitas atau kondisi dimana terdapatnya tingkat korelasi yang tinggi antara variabel independen dalam model penelitian, dengan membandingkan nilai VIF yang dimana nilai yang didapat harus lebih kecil dari pada 5, atau bahkan lebih baik lagi apabila nilai yang didapat lebih kecil daripada 3 (Hair et al., 2022). Pada **Tabel 6** merupakan hasil dari uji multikolinier pada Smartpls 4 yang dimana pada **Tabel 6** menunjukan bahwa tiap dari masing-masing variabel independen memiliki nilai VIF lebih kecil dari 2, sehingga menunjukan **tidak adanya variabel yang memiliki kolinear yang tinggi satu sama** lain dan struktur model berada pada tingkat kolinearitas yang baik karena nilai Inner VIF variabel bahkan **lebih kecil** daripada 3.

Tabel 6. Hasil Uji Multikolinier

Variabel	VIF
CIP -> SB	1.299
CTA -> PT	1.455
EPB -> SB	1.168
PS -> PT	1.213
PT -> CIP	1.146
PT -> SB	1.129
SA -> CIP	1.146
SA -> PT	1.237
SA -> SEIS	1.000
SEIS -> EPB	1.000

Uji Kebaikan Model(Model Fit)

Uji kebaikan Model (Model Fit) atau uji dengan menggunakan R-Squared (R^2) merupakan pengukuran statistik dalam menentukan proposisi dari variabel dependen penelitian yang didapat atau dijelaskan oleh variabel independen. Pengujian R-Squared menggunakan nilai koefisien determinasi(R^2) dengan batas nilai 0,75 menunjukan bahwa

model dari variabel memiliki pengaruh yang Kuat, 0,50 menunjukan bahwa model dari variabel memiliki pengaruh yang Medium atau Moderat, dan 0,25 menunjukan bahwa model dari variabel memiliki pengaruh yang Lemah (Dedi & Rianto Rahadi, 2023). Namun dalam beberapa studi nilai koefisien determinasi (R^2) juga dapat menggunakan nilai 0,10 sebagai standar dalam uji kebaikan model Ada juga yang menggunakan standar 0,65 dalam menguji kebaikan dari model variabel penelitian (Hair et al., 2022).

Nilai dari R^2 merupakan penilaian dari fungsi jumlah konstruk variabel prediktor dalam menilai atau mempengaruhi variabel dependen, dengan keadaan semakin banyak jumlah variabel yang menjadi prediktor dari variabel dependen tersebut maka nilai R2 semakin tinggi. Sehingga penginterpretasian dari nilai R2 dibuat sesuai dengan konteks penelitian dan model terkait yang digunakan dalam penelitian tersebut(Hair et al., 2022).

Pengujian R2 dalam penelitian ini akan menggunakan nilai dari R2 dalam menjelaskan tingkat persentase kekuatan dari variabel Prediktor Penelitian dalam mempengaruhi atau memprediksi perubahan yang didapat dari variabel dependen apabila variabel prediktor mendapat perubahan. Hasil dalam pengujian kebaikan model (Model Fit) dapat dilihat pada **Tabel 7**.

Tabel 7. Hasil Uji Kebaikan Model (Model Fit)

Variabel	R-square	R-square adjusted
CIP	0.134	0.117
EPB	0.109	0.101
PT	0.221	0.197
SB	0.234	0.210
SEIS	0.098	0.089

Dari hasil yang didapat dalam pengujian kebaikan model(Model Fit) didaptlah:

a. Nilai R2 variabel CIP atau Concern for Information Privacy adalah sebesar 0,134. Nilai R2 ini menjelaskan bahwa kekuatan variabel *Security Awareness(SA), Perceived Security Threat (PT), Perceived Susceptibility /Perceived Severity (PS),* dan *Cues to Action (CTA),* Dalam memprediksi *Concern for Information Privacy* adalah 13,4%. Termasuk dalam kategori pengaruh yang lemah.
b. Nilai R2 variabel EPB atau *Expectations (Perceived Benefits–Perceived Barriers)* adalah sebesar 0,109. Nilai R2 ini menjelaskan bahwa kekuatan variabel *Security Awareness(SA),* dan *Self–efficacy in Information Security(SEIS*), dalam memprediksi nilai EPB atau *Expectations (Perceived Benefits–Perceived Barriers)* adalah sebesar 10,9%. Tingkat Explanatory Power merupakan kategori Lemah.
c. Nilai R2 variabel PT atau *Perceived Security Threat* adalah sebesar 0,221. Nilai R2 ini menjelaskan bahwa kekuatan variabel prediktor *Security Awareness(SA), Cues to Action (CTA), dan Perceived Susceptibility /Perceived Severity (PS)*, dalam memprediksi PT atau *Perceived Security Threat* adalah sebesar 22,1%. Termasuk dalam kategori pengaruh yang lemah.
d. Nilai R2 variabel SEIS atau *Self–efficacy in Information Security* adalah sebesar 0,098. Nilai R2 ini menjelaskan bahwa kekuatan variabel *Security*

Awareness(SA) dalam mempengaruhi atau memprediksi variabel SEIS atau *Self–efficacy in Information Security* adalah sebesar 9,8% Termasuk dalam kategori pengaruh yang lemah, terlebih dengan hanya memiliki 1 variabel prediktor.

e. Nilai R2 variabel SB atau *Security Behavior* adalah sebesar 0.234. Nilai R2 ini menjelaskan bahwa kekuatan variabel *Security Awareness(SA), Self–efficacy in Information Security(SEIS), Expectations (Perceived Benefits–Perceived Barriers)(EPB), Concern for Information Privacy(CIP), Perceived Susceptibility /Perceived Severity (PS), Perceived Security Threat(PT*), dan *Cues to Action (CTA),* adalah sebesar 23,4%. Termasuk dalam kategori pengaruh yang lemah, walau termasuk kedalam kategori yang lemah, variabel SB atau *Security Behavior* merupakan Variabel dependen dengan variabel prediktor terbanyak dengan jumlah 7 variabel prediktor dan menunjukkan bahwa perubahan dari setiap variabel pada model dapat memberikan pengaruh pada variabel dependen SB atau *Security Behavior*.

Uji Hipotesis(*Path Coefficients*)

Pengujian hipotesis atau pengujian koefisien jalur dilakukan dengan menggunakan fitur bootstrapping, bootstrapping digunakan karena prosedur bootstrapping dalam membantu menemukan penilaian terhadap suatu indikator formatif berkontribusi secara signifikan terhadap konstruknya. Prosedur bootstrapping juga dapat membantu dalam perhitungan penemuan Nilai T (T value) dan Nilai P (P Value) yang akan digunakan dalam penentuan terhadap signifikansi dan ditolak atau diterimanya hipotesis dalam penelitian(Hair et al., 2022).

Nilai P dalam pengujian hipotesis merupakan penilaian tingkat terhadap probabilitas penolakan hipotesis 0 (H0). Dalam penelitian ini menggunakan tingkat signifikansi ($\alpha = 10\%$), sehingga nilai dari P value harus lebih kecil dari pada 0,1 sehingga dapat menerima hasil dari hipotesis penelitian (H1). Sedangkan untuk Nilai T (T value) nilai T harusnya lebih dari Nilai Kritikal (Critical value) Nilai T, dengan tingkat signifikansi 10% nilai kritikal yang dibandingkan adalah 1,65. Sehingga nilai T harusnya lebih besar dari pada 1,65 agar dapat dikatakan memiliki pengaruh hubungan yang signifikan pada penelitian(Dedi & Rianto Rahadi, 2023; Hair et al., 2022). Pengujian Hipotesis atau koefisien jalur dengan menggunakan SmartPLS 4 juga bisa mendapatkan hasil terkait efek langsung dan tidak langsung yang didapat oleh variabel. Hasil dari pengujian koefisien jalur ini dapat dilihat pada **Tabel 8**.

Tabel 8 Hasil Pengujian Koefisien Jalur

Hipotesis	Hipotesis	T Value	P Value	Direct Effect
H1	SA -> SEIS	1.942	0.052	0.313
H2	SA -> CIP	1.037	0.300	0.020
H3	SA -> PT	2.523	0.012	0.329
H4	SEIS -> EPB	1.933	0.053	0.331
H5	CIP -> SB	0.141	0.888	0.020
H6	PT -> CIP	1.932	0.053	0.284
H7	PS -> PT	1.434	0.152	0.278
H8	CTA -> PT	0.393	0.694	0.060

H9	EPB -> SB	1.717	0.086	0.227
H10	PT -> SB	2.429	0.015	0.389

Hasil yang didapat dari **Tabel 8** didapat penjelasan sebagai berikut:

a. **Hipotesis 1**, Adanya hubungan yang signifikan terhadap kesadaran privasi terhadap keamanan (*Security Awareness*) (SA) data pemain dalam memahami praktik keamanan informasi (*Self-Efficacy in Information Security*) (SEIS) pemain game gacha. Dengan pengaruh langsung yang diberikan *Security Awareness* (SA) terhadap *Self-Efficacy In Information Security* (SEIS) adalah 0,313. Hubungan bersifat Positif dan Hal ini juga menunjukan apabila terjadi kenaikan nilai pada variabel *Security Awareness* (SA), akan terjadi kenaikan nilai sebesar 31,3% pada *Self-Efficacy In Information Security* (SEIS).
b. **Hipotesis 2**, Tidak adanya hubungan dan tidak signifikannya hubungan kesadaran privasi terhadap keamanan (*Security Awareness*) (SA) terhadap tingkat perhatian pemain terhadap informasi data yang mereka berikan ketika berinteraksi terlebih dalam praktik privasi informasi (*Concern for Information Privacy*) (CIP). Direct effect yang dimiliki hubungan ini bersifat positif dan pengaruh sebesar 0,020 atau 2%.
c. **Hipotesis 3**, Adanya Hubungan yang signifikan kesadaran privasi terhadap keamanan (*Security Awareness*) (SA)pada kemampuan persepsi Pemain terhadap ancaman keamanan (*Perceived Security Threat*) (PT). Dengan Total Direct effect sebesar 0,329 menunjukan hubungan yang bersifat positif, dengan pengaruh yang dapat diberikan *Security Awareness* (SA) pada *Perceived Security Threat* (PT) adalah sebesar 32,9%.
d. **Hipotesis 4**, Adanya hubungan yang signifikan terhadap pengetahuan Pemain dalam memahami praktik keamanan informasi (*Self-Efficacy In Information Security*) (SEIS) dan harapan Pemain (*Expectations Perceived Benefits–Perceived Barriers*) (EPB) terhadap harapan akan manfaat yang akan mereka dapat atau bahkan ekspektasi pemain terhadap hambatan yang mungkin didapat dalam praktik keamanan informasi data akun mereka. Total Direct effect sebesar 0,331, hubungan yang dimiliki bersifat Positif dengan pengaruh yang diberikan *Self-Efficacy In Information Security* (SEIS) pada *Expectations Perceived Benefits–Perceived Barriers* (EPB) adalah sebesar 33,1%
e. **Hipotesis 5**, Tidak adanya hubungan yang signifikan terhadap tingkat perhatian pemain terhadap informasi data yang mereka berikan ketika berinteraksi terlebih dalam praktik privasi informasi (*Concern For Information Privacy*) (CIP) dalam praktik perilaku keamanan dari pemain (*Security Behavior*) (SB). Total Direct effect sebesar 0,020, hubungan bersifat positif dengan pengaruh pada hubungan ini hanya sebesar 2%.
f. **Hipotesis 6**, Signifikannya Hubungan persepsi Pemain terhadap ancaman keamanan (*Perceived Security Threat*) (PT) terhadap tingkat kewajaran Pemain dalam berinteraksi dan pada saat bermain terlebih dalam praktik privasi informasi personal informasi (*Concern for Information Privacy*) (CIP). Total Direct effect sebesar 0,284, hubungan variabel bersifat positif dengan pengaruh *Perceived Security Threat* (PT) dapat mempengaruhi *Concern for Information Privacy* (CIP) sebesar 28,4%
g. **Hipotesis 7**, Tidak terdapatnya hubungan yang signifikan antara persepsi kelemahan/persepsi keparahan (*Perceived Susceptibility/Perceived Severity*) (PS) dan persepsi Pemain terhadap ancaman keamanan (*Perceived Security Threat*) (PT). walau dari hasil pengujian nilai T didapat bahwa tidak adanya hubungan yang signifikan yang

dimiliki, Total Direct effect sebesar 0,278 masih menunjukan pengaruh perubahan yang ada pada hubungan jalur ini adalah 27,8%. Hubungan bersifat Positif.

h. **Hipotesis 8**, Tidak terdapatnya hubungan terhadap aktivitas yang dapat memotivasi pemain untuk merubah perilaku Pemain (*Cues To Action*) (CTA) pada persepsi Pemain terhadap ancaman keamanan (*Perceived Security Threat*) (PT). Total Direct effect sebesar 0,060, hubungan yang ditunjukan bersifat positif, dengan besar pengaruh yang ada pada hubungan ini hanya sebesar 6%.
i. **Hipotesis 9**, Signifikannya Hubungan pada ekspektasi dan harapan Pemain (persepsi kemanfaatan–persepsi hambatan (*Expectations Perceived Benefits–Perceived Barriers*) (EPB) terhadap efek yang diberikan pada perilaku keamanan (*Security Behavior*) (SB) dalam melindungi informasi akun game pemain. Total Direct effect sebesar 0,227, hubungan bersifat positif, pengaruh yang diberikan *Expectations Perceived Benefits–Perceived Barriers* (EPB) akan mempengaruhi *Security Behavior* (SB) sebesar 22,7%
j. **Hipotesis 10**, Adanya hubungan yang signifikan terhadap kemampuan persepsi pemain terhadap ancaman keamanan (*Perceived Security Threat*) (PT) dalam mempengaruhi perilaku keamanan (*Security Behavior*) (SB) pemain dalam melindungi privasi informasi akun game pemain. Total Direct effect sebesar 0,389, menunjukan hubungan variabel bersifat positif dengan pengaruh yang diberikan *Perceived Security Threat* (PT) pada *Security Behavior* (SB) adalah 38,9%.

Selain hubungan langsung, adapun hubungan tidak langsung yang bisa didapat dari uji hipotesis koefisien jalur, sebagaimana yang didapat pada **Tabel 9**. Dengan mempertimbangkan nilai P value, dan T value. Didapat lah hasil dimana terdapatnya hubungan yang signifikan pada *Security Awareness* (SA) terhadap perilaku pemain dalam menjaga privasi data akun game mereka (*Security Behavior*) (SB). Dengan nilai Indirect effect 0,156, menandakan hubungan yang dimiliki bersifat positif dengan *Security Awareness* (SA) dapat memberi perubahan secara pengaruh tidak langsung kepada variabel *Security Behavior* (SB) sebesar 15,6%.

Tabel 9. Hasil Indirect Effect

Hubungan	T Value	P Value	Indirect Effect
SA -> SB	2.165	0.030	0.156

Penelitian ini menunjukkan bahwa *Security Awareness* (SA) berpengaruh signifikan dalam meningkatkan *Self-efficacy* (SEIS) dan *Perceived Security Threat* (PT) pada pemain Genshin Impact dan Wuthering Waves. Tingginya kewaspadaan membuat pemain lebih percaya diri dalam mengidentifikasi ancaman seperti phishing serta lebih selektif dalam memilih layanan pihak ketiga (top-up atau joki). Meskipun SA tidak berpengaruh langsung terhadap kepedulian privasi (CIP), variabel ini mampu memengaruhi CIP secara tidak langsung melalui pemahaman ancaman (PT). Menariknya, ditemukan bahwa meskipun pemain memiliki kesadaran tinggi, mereka cenderung masih meremehkan risiko privasi jika tidak memahami eskalasi ancaman tersebut secara spesifik.

Di sisi lain, perilaku keamanan pemain (*Security Behavior*/SB) secara signifikan didorong oleh *Expectations* (EPB) dan pemahaman akan ancaman (PT), namun tidak

dipengaruhi oleh tingkat kepedulian privasi (CIP). Hal ini mengindikasikan bahwa pemain akan mengambil tindakan pengamanan data selama mereka memahami manfaat, hambatan, dan risiko nyata yang dihadapi, tanpa harus memiliki rasa peduli yang mendalam terhadap privasi itu sendiri. Kepercayaan diri dalam mengamankan data (SEIS) juga terbukti memperkuat ekspektasi pemain terhadap hasil dari tindakan keamanan yang mereka lakukan, sehingga meminimalisir potensi dampak negatif pada akun mereka.

4. Kesimpulan dan Saran

Kesimpulan

Hasil yang diberikan setelah pengujian Hipotesis dengan menggunakan koefisien jalur dan mendapatkan hasil dari *Direct Effect* dan *Indirect Effect,* didapatlah penjelasan terhadap efek yang diberikan variabel. Seperti efek variabel *Security Awareness* dalam mempengaruhi *Self-Efficacy in Information Security* dan *Perceived Security Threat*, dimana banyak dari pemain menyadari bahaya yang ada terhadap keamanan privasi data mereka, hal ini mempengaruhi kekhawatiran dan tingkat kecemasan pemain terhadap ancaman yang mungkin saja akan mereka temukan. Selain hal tersebut, banyak pemain akan mencari informasi lebih lanjut sebelum menggunakan layanan joki maupun Top-up, dengan hal tersebut pemain merasa percaya diri dalam melindungi akun mereka dan memilih layanan jasa joki dan top-up yang dapat dipercaya.

Adapun pengaruh variabel *Self-Efficacy in Information Security* terhadap *Expectations Perceived Benefits–Perceived Barriers*, dimana dari hubungan tersebut menunjukan tingkat kepercayaan diri pemain dalam memilih layanan jasa yang akan mereka gunakan dapat dipastikan aman dan terpercaya pada saat menggunakan layanan tersebut. *Expectations Perceived Benefits–Perceived Barriers* juga mempengaruhi variabel *Security Behavior.* Dimana dengan menyadari akan manfaat dan hambatan yang akan mereka dapatkan dalam usaha mereka menjaga privasi data mereka, pemain cenderung mengambil tindakan pencegahan untuk menghindari ancaman tersebut, seperti menghindari link dari chat asing yang mencurigakan dan tidak sembarangan menggunakan layanan top-up dan joki.

Variabel *Perceived Security Threat* juga mempengaruhi *Security Behavior*. Dimana dengan perasaan khawatir dan kecemasan pemain apabila mereka kehilangan akun game mereka, pemain game Genshin Impact dan Wuthering Waves cenderung lebih berhati-hati dan tidak sembarangan dalam menyebarkan informasi akun mereka, dan guna menghindari ancaman phising dan scam, pemain juga akan menghindari chat berisikan link mencurigakan yang berasal dari pemain asing pada saat bermain.

Terakhir, berdasarkan pengaruh tidak langsung yang dapat diberikan variabel *Security Awareness* terhadap *Security Behavior*. Pemain yang mengetahui ancaman privasi data cenderung akan lebih bersikap hai-hati dan dapat mengambil tindakan guna menjaga dan memastikan keamanan terhadap privasi data mereka.

Penelitian ini menunjukkan bahwa *Security Awareness* (SA) berpengaruh signifikan dalam meningkatkan *Self-efficacy* (SEIS) dan *Perceived Security Threat* (PT) pada pemain Genshin Impact dan Wuthering Waves. Tingginya kewaspadaan membuat pemain lebih percaya diri dalam mengidentifikasi ancaman seperti phishing serta lebih selektif dalam memilih layanan pihak ketiga (top-up atau joki). Meskipun SA tidak berpengaruh langsung terhadap kepedulian privasi (CIP), variabel ini mampu memengaruhi CIP secara tidak langsung melalui pemahaman ancaman (PT). Menariknya, ditemukan bahwa meskipun pemain memiliki kesadaran tinggi, mereka cenderung masih meremehkan risiko privasi jika tidak memahami eskalasi ancaman tersebut secara spesifik.

Di sisi lain, perilaku keamanan pemain (*Security Behavior*/SB) secara signifikan didorong oleh *Expectations* (EPB) dan pemahaman akan ancaman (PT), namun tidak dipengaruhi oleh tingkat kepedulian privasi (CIP). Hal ini mengindikasikan bahwa pemain akan mengambil tindakan pengamanan data selama mereka memahami manfaat, hambatan, dan risiko nyata yang dihadapi, tanpa harus memiliki rasa peduli yang mendalam terhadap privasi itu sendiri. Kepercayaan diri dalam mengamankan data (SEIS) juga terbukti memperkuat ekspektasi pemain terhadap hasil dari tindakan keamanan yang mereka lakukan, sehingga meminimalisir potensi dampak negatif pada akun mereka.

Adapun saran yang didapat dalam melakukan penelitian ini adalah penelitan berikutnya dapat melakukan penelitian pada bidang game, tema game, atau game yang berbeda untuk mendapatkan perspektif dari game dan pemain dari bidang, tema atau game tersebut.selain itu penelitian berikutnya dapat menggunakan tingkat signifikansi (α) yang lebih kecil seperti tingkat signifikansi 5% atau bahkan tingkat signifikansi 1% guna mendapatkan hasil yang lebih baik. Dan terakhir apabila terdapat seminar tentang privasi data, diharapkan dapat membawa materi tentang ancaman yang ada pada bidang video game, dan berfokus pada *Security Awareness, Self-Efficacy in Information Security, Expectations (Perceived Benefits–Perceived Barriers), Perceived Security Threat, Security Behavior*

Daftar Pustaka

Aisisoda. (2024). Scam Akun Top Up Gratis di Genshin Impact. In *Tiktok*.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *ArXiv Preprint ArXiv:1901.02672*. https://arxiv.org/abs/1901.02672

BetaNebula. (2023, June 15). *EVERYONE BE AWARE OF A NEW TYPE OF SCAM!!* . Hoyolab. https://www.hoyolab.com/article/19370494

Borgo, R., Marai, G. E., Schreck, T., South, L., Saffo, D., Vitek, O., Dunne, C., & Borkin, M. A. (2022). Effective Use of Likert Scales in Visualization Evaluations: A Systematic Review. In *EuroVis)* (Vol. 2022, Issue 3). https://osf.io/exbz8/.

Chen, C., & Fang, Z. (2023). Gacha Game Analysis and Design. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *7*(1). https://doi.org/10.1145/3579438

Dedi, R., & Rianto Rahadi, D. (2023). *PENGANTAR PARTIAL LEAST SQUARES STRUCTURAL EQUATION MODEL(PLS-SEM) 2023*. https://www.researchgate.net/publication/372827232

Dewi, F. K. S., & Natalia, B. (2021). Identifying the Factors of Online Game Acceptance Using Technology Acceptance Model. In *Indonesian Journal of Information Systems (IJIS* (Vol. 4, Issue 1). https://doi.org/10.24002/ijis.v4i1.4727

Du, J., Kalafut, A., & Schymik, G. (2024). The health belief model and phishing: determinants of preventative security behaviors. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyae012

Edwards, K. (2015). *NSUWorks Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users* [Nova Southeastern University]. https://nsuworks.nova.edu/gscis_etd/947/

Fathni, I., Zulaika, S., & Sari Dewi, R. (n.d.). *Pengaruh Kebijakan Privasi, dan Tingkat Kepercayaan Pada Platform Digital terhadap Perilaku Pengguna dalam Melindungi Privasi Online di Indonesia Article Info ABSTRAK*. *2*(02), 118–126. https://doi.org/10.58812/shh.v2.i02

Garland, R. (1991). The Mid-Point on a Rating Scale: Is it Desirable? In *Marketing Bulletin* (Vol. 2). http://marketing-bulletin.massey.ac.nz

Hair, J., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2022). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. https://www.researchgate.net/publication/354331182_A_Primer_on_Partial_Least_Squares_Structural_Equation_Modeling_PLS-SEM

Haulussy, F. (2024, October 11). *Apa yang Membuat Game Gacha Begitu Populer?* GAMEFINITY. https://www.gamefinity.id/game/apa-yang-membuat-game-gacha-begitu-populer/

Jacked Yuan. (2025, May 13). *Gacha revenue May 2025 (mobile platforms only)*. Hoyolab. https://www.hoyolab.com/article/38770082

Kusmaryono, I., Wijayanti, D., & Maharani, H. R. (2022). Number of Response Options, Reliability, Validity, and Potential Bias in the Use of the Likert Scale Education and Social Science Research: A Literature Review. In *International Journal of Educational Methodology* (Vol. 8, Issue 4, pp. 625–637). Eurasian Society of Educational Research. https://doi.org/10.12973/ijem.8.4.625

Muhammad Naufal, F. (2024). *EVALUASI KESADARAN MAHASISWA UNIVERSITAS JAMBI TERHADAP PRIVASI DATA PRIBADI DARI BAHAYA PHISHING* [Thesis (S1), Universitas Jambi]. https://repository.unja.ac.id/id/eprint/71073

Permana, R. R., & Rakhmawati, N. A. (2023). ANALISIS KESADARAN PRIVASI TERHADAP TREN DI MEDIA SOSIAL PADA MAHASISWA SISTEM INFORMASI ITS. In *Etika Teknologi Informasi Semester Genap*. https://doi.org/10.13140/RG.2.2.10099.54567

Pertiwi, T. K., Purwanto, E., Kusuma, I. D., Dewi, S., & Kisdayanti, L. (n.d.). *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS Impact of Perceived Benefits, Security, and Privacy on Interest in Using E-Wallet in Millennial Generation*. https://doi.org/10.47191/ijmra/v5-i5-22

Priadana, M. S., & Sunarsi, D. (2021). *Metode penelitian kuantitatif*. Pascal Books. https://anyflip.com/tzxmy/fzxh

Toto, Dr. S. (2021). *Gacha: Explaining Japan's Top Money-Making Social Game Mechanism.* . https://www.serkantoto.com/2012/02/21/gacha-social-games/.

Williams, C., Wynn, D., Karahanna, M. R., & Duncan. (2014). *"Explaining Users Security Behavior with the Security Belief Model," forthcoming at the Journal of Organizational Computing and Electronic Commerce. Explaining Users' Security Behaviors with the Security Belief Model*. https://doi.org/10.4018/joeuc.2014070102

Zahwani[1], S. T., Irwan, M., & Nasution[2], P. (2023). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. *Analisis Kesadaran Masyarakat (Zahwani, Dkk.) JoSES: Journal of Sharia Economics Scholar*, *2*(2), 105–109. https://doi.org/10.5281/zenodo.12608751