Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

ANALISIS PERILAKU KEAMANAN INFORMASI PENGGUNA APLIKASI *SHOPEE* MENGUNAKAN *FRAMEWORK SECURITY BEHAVIOR INTENTIONS SCALE (SeBIS)*

Yufentus Leokuna[1], Sintaria Sembiring[2]
1,2) Fakultas Teknologi Informasi, Universitas Advent Indonesia

Article Info

Article history:

Received: 08 Maret 2026
Revised: 24 Maret 2026
Accepted: 29 Maret 2026

ABSTRACT

Abstrak

Perkembangan teknologi digital mendorong peningkatan penggunaan e-commerce yang mempermudah transaksi online, namun juga meningkatkan risiko terhadap keamanan informasi pribadi pengguna. Penelitian ini bertujuan untuk menganalisis tingkat perilaku keamanan informasi pengguna aplikasi Shopee di Kota Bandung menggunakan framework Security Behavior Intentions Scale (SeBIS) serta menganalisis hubungan masing-masing dimensinya terhadap perilaku keamanan informasi. Penelitian ini menggunakan pendekatan survei kuantitatif dengan instrumen kuesioner online yang mencakup empat dimensi SeBIS, yaitu proactive awareness, password generation, software updating, dan device securement. Sebanyak 251 pengguna aktif Shopee berpartisipasi dalam penelitian ini, dengan ukuran sampel ditentukan menggunakan rumus Lemeshow dengan margin of error 10%. Analisis data dilakukan melalui uji validitas, uji reliabilitas, analisis deskriptif, serta uji korelasi Pearson menggunakan perangkat lunak IBM SPSS Statistics. Hasil penelitian menunjukkan bahwa tingkat perilaku keamanan informasi pengguna Shopee di Kota Bandung berada pada kategori tinggi. Seluruh dimensi SeBIS memiliki hubungan positif dan signifikan ($p < 0,001$) terhadap perilaku keamanan informasi dengan kekuatan korelasi sangat kuat ($r = 0,854–0,902$), dimana dimensi device securement menunjukkan hubungan paling kuat terhadap perilaku keamanan informasi pengguna.

Kata Kunci: Shopee, keamanan informasi, SeBIS, e-commerce, perilaku pengguna.

Abstract

The rapid development of digital technology has increased the use of e-commerce platforms, making online transactions easier while also raising concerns regarding users' information security. This study aims to analyze the level of information security behavior of Shopee users in Bandung City using the Security Behavior Intentions Scale (SeBIS) framework and examine the relationship between each dimension and users' information security behavior. This research employed a quantitative survey approach using an online questionnaire covering four SeBIS dimensions: proactive awareness, password generation, software updating, and device securement. A total of 251 active Shopee users participated in this study, with the sample size determined using the Lemeshow formula with a 10% margin of error. Data analysis was conducted through validity testing, reliability testing, descriptive analysis, and Pearson

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

correlation analysis using IBM SPSS Statistics. The results show that the information security behavior of Shopee users in Bandung is categorized as high. All SeBIS dimensions show positive and significant relationships (p < 0.001) with information security behavior with very strong correlations (r = 0.854–0.902), where device securement has the strongest relationship..

Keywords: **Shopee, information security, SeBIS, e-commerce, user behavior.**

Corresponding Author:
E-mail : 2282013@unai.edu

1. PENDAHULUAN

Perkembangan teknologi digital telah mengubah cara masyarakat mengakses informasi dan melakukan transaksi, terutama melalui *platform e-commerce* seperti *Shopee.* Peningkatan jumlah pengguna dan transaksi online membawa kemudahan dalam berbelanja, namun di sisi lain juga meningkatkan potensi risiko terhadap keamanan informasi pribadi pengguna. Kepercayaan pengguna, perlindungan data, serta keamanan dalam berinteraksi menjadi faktor. penting yang memengaruhi keputusan bertransaksi pada *platform e-commerce* [1].

Shopee merupakan salah satu *platform e-commerce* terbesar di Asia Tenggara yang banyak digunakan di Indonesia. Berdasarkan laporan [10], jumlah pengguna internet di Indonesia mencapai 221 juta orang atau sekitar 79,5% dari total populasi, dengan 78,3% di antaranya melakukan aktivitas belanja online. Shopee menempati posisi teratas sebagai aplikasi *e-commerce* yang paling banyak digunakan. Kondisi ini menunjukkan bahwa semakin luasnya penggunaan platform digital juga diikuti oleh meningkatnya potensi risiko kebocoran data pribadi dan ancaman keamanan siber.

Dalam praktiknya, masih banyak pengguna e-commerce yang belum menerapkan perilaku keamanan informasi secara optimal. Beberapa kebiasaan yang berisiko antara lain penggunaan kata sandi yang sama pada berbagai akun, membagikan kode OTP kepada pihak lain, tidak memperbarui aplikasi secara berkala, serta melakukan transaksi melalui jaringan Wi-Fi publik yang tidak aman. Selain itu, maraknya kasus phishing, tautan promosi palsu, dan akun *Shopee* palsu di media sosial menunjukkan bahwa kesadaran keamanan digital pengguna masih perlu ditingkatkan [16], [17]. Laporan [18] juga menunjukkan bahwa lebih dari 50% pengguna internet di Asia Tenggara masih menggunakan kata sandi yang lemah dan jarang melakukan pembaruan sistem keamanan.

Sejumlah penelitian sebelumnya menekankan pentingnya keamanan informasi dalam konteks e-commerce. Penelitian [3] menunjukkan bahwa keamanan informasi berpengaruh terhadap loyalitas pelanggan karena meningkatkan rasa

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

aman dan kepercayaan saat bertransaksi. Penelitian [4] menyatakan bahwa tingkat kepercayaan terhadap sistem keamanan aplikasi memengaruhi keputusan pembelian pengguna *Shopee.* Selain itu, [5] menemukan bahwa persepsi risiko dan kepercayaan terhadap sistem keamanan berhubungan dengan niat pengguna dalam berinteraksi secara online.

Untuk mengukur perilaku keamanan informasi secara sistematis, salah satu instrumen yang banyak digunakan adalah *Security Behavior Intentions Scale (SeBIS). Framework* ini mengukur perilaku keamanan pengguna melalui empat dimensi utama, yaitu *Proactive Awareness, Password Generation, Software Updating,* dan *Device Securement.* Penelitian [6] menunjukkan bahwa individu dengan tingkat penerapan dimensi-dimensi *SeBIS* yang baik cenderung menerapkan praktik keamanan informasi secara konsisten. Meskipun demikian, penelitian yang secara khusus menganalisis perilaku keamanan informasi pengguna *Shopee* menggunakan kerangka *SeBIS* di Indonesia masih terbatas, khususnya pada konteks pengguna di Kota Bandung.

Kota Bandung merupakan salah satu kota dengan tingkat penggunaan internet dan aktivitas e-commerce yang tinggi di Provinsi Jawa Barat. Berdasarkan data [12], jumlah penduduk Kota Bandung mencapai sekitar 2,5 juta jiwa, dengan lebih dari 90% penduduk telah mengakses internet dalam tiga bulan terakhir. Selain itu, wilayah Jawa Barat termasuk salah satu pasar terbesar *Shopee* di Indonesia [11]. Hal ini menjadikan Kota Bandung sebagai lokasi yang relevan untuk meneliti perilaku keamanan informasi pengguna *Shopee.*

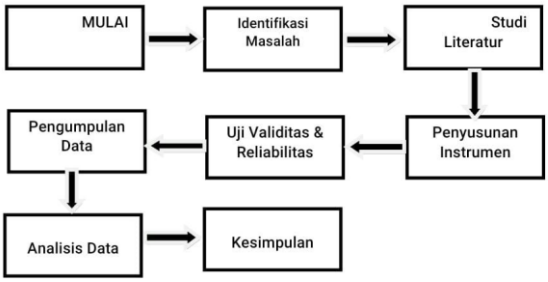
Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis tingkat perilaku keamanan informasi pengguna aplikasi *Shopee* di Kota Bandung menggunakan *framework Security Behavior Intentions Scale (SeBIS)*, serta menganalisis pengaruh masing-masing dimensi *SeBIS (Proactive Awareness, Password Generation, Software Updating, Device Securement)* terhadap perilaku keamanan informasi pengguna. Penelitian ini diharapkan dapat memberikan gambaran mengenai praktik keamanan digital pengguna *e-commerce*, serta menjadi dasar dalam meningkatkan kesadaran dan literasi keamanan informasi, dengan memperhatikan kontribusi masing-masing dimensi SeBIS terhadap perilaku keamanan pengguna.

2. METODE PENELITIAN

a. Tahapan Penelitian

Tahapan penelitian dalam studi ini disusun secara sistematis untuk memperoleh data yang valid dan reliabel. Alur tahapan penelitian ditunjukkan pada Gambar .1

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno



Gambar 2.1 menunjukkan langkah-langkah penelitian yang dilakukan mulai dari identifikasi masalah, pengumpulan data, analisis data, hingga penarikan kesimpulan.

b. Design Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei untuk menganalisis perilaku keamanan informasi pengguna aplikasi Shopee di Kota Bandung. Pendekatan ini memungkinkan pengukuran variabel secara sistematis dan objektif melalui instrumen penelitian yang terstandarisasi.

Instrumen penelitian menggunakan Security Behavior Intentions Scale (SeBIS) yang terdiri dari empat dimensi, yaitu Proactive Awareness, Password Generation, Software Updating, dan Device Securement. Kuesioner disebarkan secara daring kepada pengguna aktif Shopee di Kota Bandung yang telah melakukan transaksi dalam tiga bulan terakhir.

Data yang diperoleh dianalisis menggunakan uji validitas dan reliabilitas untuk memastikan kualitas instrumen. Selanjutnya dilakukan analisis deskriptif untuk mengetahui tingkat perilaku keamanan informasi pengguna serta uji korelasi Pearson untuk menganalisis hubungan antara dimensi SeBIS (X_1–X_4) dengan perilaku keamanan informasi (Y).

c. Variabel Penelitian dan Definisi Operasional

Penelitian ini menggunakan konstruk perilaku keamanan informasi yang diukur berdasarkan framework Security Behavior Intentions Scale (SeBIS). Dalam penelitian ini, dimensi SeBIS digunakan sebagai variabel independen (X), sedangkan perilaku keamanan informasi digunakan sebagai variabel dependen (Y).

Perilaku keamanan informasi didefinisikan sebagai tindakan pengguna dalam melindungi data pribadi, akun, serta aktivitas transaksi daring dari potensi ancaman digital seperti penipuan, kebocoran data, dan akses tidak sah. Konstruk ini diukur melalui empat dimensi utama dalam framework SeBIS [6], yaitu Proactive Awareness, Password Generation, Software Updating, dan Device Securement.

Keempat dimensi tersebut dianalisis secara deskriptif untuk mengetahui tingkat perilaku keamanan informasi pengguna. Selanjutnya, hubungan antara masing-masing dimensi SeBIS (X_1–X_4) dengan perilaku keamanan informasi (Y) dianalisis menggunakan uji korelasi Pearson.

Tabel berikut menjelaskan definisi operasional dan indikator masing-masing variabel.

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Variabel Independen	Kode	Definisi Operasional	Indikator Utama
Kesadaran Keamanan (Proactive Awareness)	X_1	Tingkat perhatian pengguna terhadap tanda-tanda keamanan digital saat bertransaksi di Shopee.	Menghindari tautan mencurigakan, memperhatikan HTTPS/gembok, membaca kebijakan privasi.
Pengelolaan Kata Sandi (Password Generation)	X_2	Kebiasaan pengguna dalam menciptakan dan mengelola kata sandi yang kuat serta aman.	Menggunakan kombinasi karakter kuat, tidak menggunakan kata sandi yang sama di akun lain, mengganti kata sandi secara berkala.
Pembaruan Perangkat Lunak (Software Updating)	X_3	Tingkat konsistensi pengguna dalam memperbarui aplikasi Shopee dan sistem perangkat untuk menjaga keamanan.	Memperbarui aplikasi Shopee, menjaga versi terbaru sistem, mengaktifkan pembaruan otomatis.
Keamanan Perangkat (Device Securement)	X_4	Upaya pengguna dalam melindungi perangkat dari akses tidak sah saat menggunakan aplikasi Shopee.	Mengunci layar perangkat, menggunakan PIN/biometrik, melakukan logout setelah penggunaan.
Variabel Dependen	**Kode**	**Definisi Operasional**	**Indikator Utama**
Perilaku Keamanan Informasi	Y	Tingkat keseluruhan perilaku pengguna dalam melindungi data pribadi, akun, serta aktivitas transaksi daring dari potensi ancaman digital.	Dinyatakan melalui keseluruhan item pada keempat dimensi SeBIS: Proactive Awareness, Password Generation, Software Updating, dan Device Securement.

a. ***Security Behavior Intentions Scale (SeBIS)***

Security Behavior Intentions Scale (SeBIS) adalah framework yang terdiri dari beberapa dimensi yang mencakup pengetahuan, sikap, dan niat perilaku yang berkaitan dengan keamanan informasi, yang dirancang untuk mengukur niat perilaku keamanan informasi individu. Framework ini digunakan dalam penelitian ini karena dapat membantu mengidentifikasi faktor-faktor (X_1–X_4) yang memengaruhi perilaku keamanan informasi (Y) pengguna aplikasi Shopee [8].

Dalam konteks aplikasi Shopee, SeBIS digunakan untuk menilai pengetahuan dan kesadaran pengguna terhadap risiko yang terkait dengan keamanan data pribadi dan transaksi online. Misalnya, pengguna yang memiliki kesadaran tinggi terhadap praktik keamanan cenderung lebih berhati-hati dalam membagikan informasi pribadi dan lebih konsisten menggunakan fitur keamanan yang tersedia di aplikasi. Penelitian sebelumnya menunjukkan bahwa pengetahuan dan persepsi individu tentang keamanan memiliki pengaruh signifikan terhadap niat individu untuk berperilaku aman [9].

Selain itu, SeBIS juga mempertimbangkan faktor-faktor eksternal, seperti lingkungan dan budaya, yang dapat memengaruhi pilihan perilaku keamanan. Penelitian ini meneliti bagaimana dimensi-dimensi SeBIS (X_1–X_4) saling terkait dan memengaruhi perilaku keamanan informasi (Y) pengguna Shopee dalam melindungi data pribadi dan aktivitas transaksi daring.

d. Metode Pengumpulan Data

Data penelitian diperoleh melalui kuesioner online yang disebarkan menggunakan Google Forms dan media sosial. Instrumen penelitian menggunakan kuesioner adaptasi dari Security Behavior Intentions Scale (SeBIS) yang dikembangkan oleh [6]. Kuesioner telah diterjemahkan ke dalam Bahasa Indonesia menggunakan metode forward translation dan back translation untuk menjaga kesesuaian makna, serta disesuaikan dengan konteks penggunaan aplikasi Shopee.

Kuesioner terdiri dari dua bagian, yaitu data demografi dan skala SeBIS. Data demografi meliputi umur, gender, domisili, lama penggunaan Shopee, serta frekuensi

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

penggunaan Shopee dalam satu bulan. Skala SeBIS digunakan untuk mengukur perilaku keamanan informasi melalui empat dimensi, yaitu Proactive Awareness, Password Generation, Software Updating, dan Device Securement yang terdiri dari 15 indikator pernyataan.

Setiap pernyataan menggunakan skala Likert 5 poin dengan pilihan jawaban: sangat tidak setuju (1), tidak setuju (2), netral (3), setuju (4), dan sangat setuju (5).

e. Populasi dan Sampel

1) Populasi

Populasi dalam penelitian ini adalah pengguna aktif aplikasi Shopee yang berdomisili di Kota Bandung dan telah melakukan transaksi pembelian dalam tiga bulan terakhir. Kota Bandung dipilih karena tingginya tingkat penggunaan internet dan aktivitas e-commerce. Berdasarkan data [13], lebih dari 90% penduduk berusia di atas 5 tahun telah mengakses internet dalam tiga bulan terakhir, sementara laporan [10] menunjukkan bahwa 78,3% pengguna internet di Indonesia melakukan belanja daring dengan Shopee sebagai salah satu platform yang paling banyak digunakan. Karena tidak terdapat data resmi mengenai jumlah pengguna aktif Shopee di Kota Bandung, maka populasi penelitian tidak diketahui secara pasti.

2) Sampel dan Teknik Pengambilan Sampel

Teknik pengambilan sampel menggunakan purposive sampling, yaitu pemilihan responden berdasarkan kriteria tertentu. Kriteria responden meliputi berdomisili di Kota Bandung, merupakan pengguna aktif Shopee yang telah melakukan minimal satu transaksi dalam tiga bulan terakhir, serta berusia antara 15 hingga 30 tahun.

Jumlah sampel ditentukan menggunakan metode Lemeshow karena populasi tidak diketahui secara pasti [13]. Hasil perhitungan menunjukkan jumlah sampel minimum sebesar 96 responden. Untuk mengantisipasi data yang tidak lengkap, penelitian menetapkan minimal 100 responden. Dalam pelaksanaannya, penelitian berhasil memperoleh data dari 251 responden yang memenuhi kriteria penelitian.

f. Uji Validitas

Uji validitas dilakukan menggunakan korelasi Pearson Product Moment untuk mengetahui kemampuan setiap item pernyataan dalam mengukur konstruk penelitian. Item dinyatakan valid apabila nilai r hitung lebih besar dari r tabel pada tingkat signifikansi 5%.

g. Uji Reliabitas

Uji reliabilitas dilakukan menggunakan metode Cronbach's Alpha untuk mengukur konsistensi internal instrumen penelitian. Instrumen dinyatakan reliabel apabila nilai Cronbach's Alpha lebih besar dari 0,70.

h. Teknik Analisis Data

Analisis data dilakukan menggunakan perangkat lunak Statistical Package for the Social Sciences (SPSS). Variabel yang dianalisis terdiri dari empat dimensi SeBIS, yaitu *Proactive Awareness (X_1), Password Generation (X_2), Software Updating (X_3), dan Device Securement (X_4),* serta perilaku keamanan informasi (Y).

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Tahapan analisis data meliputi pengolahan data, analisis deskriptif, dan uji korelasi Pearson.

1) Pengolahan Data
   Data kuesioner terlebih dahulu melalui tahap editing, coding, entry data, dan cleaning untuk memastikan kelengkapan serta ketepatan data sebelum dilakukan analisis statistik.
2) Analisis Deskriptif
   Analisis deskriptif dilakukan untuk menggambarkan tingkat perilaku keamanan informasi pengguna aplikasi Shopee pada setiap dimensi dalam Security Behavior Intentions Scale (SeBIS). Analisis ini meliputi perhitungan nilai minimum, maksimum, rata-rata (mean), dan simpangan baku (standard deviation). Melalui analisis ini dapat diketahui dimensi dengan tingkat keamanan tertinggi dan terendah, kecenderungan perilaku responden berdasarkan nilai rata-rata, serta variasi jawaban responden berdasarkan simpangan baku. Hasil analisis deskriptif selanjutnya digunakan sebagai dasar untuk melakukan analisis inferensial menggunakan uji korelasi Pearson.
3) Uji Korelasi Pearson
   Uji korelasi Pearson digunakan untuk mengetahui hubungan antara masing-masing dimensi SeBIS (X_1–X_4) dengan perilaku keamanan informasi (Y). Hubungan dinyatakan signifikan apabila nilai signifikansi kurang dari 0,05, sedangkan kekuatan hubungan ditentukan berdasarkan nilai koefisien korelasi (r).

3. HASIL DAN PEMBAHASAN

Hasil Uji Validitas

Tabel 2. Hasil Uji Validitas Instrumen

Item Pernyataan	r hitung	r tabel	Keterangan
X1.1	0,683	0,361	Valid
X1.2	0,729	0,361	Valid
X1.3	0,699	0,361	Valid
X1.4	0,664	0,361	Valid
X2.1	0,745	0,361	Valid
X2.2	0,781	0,361	Valid
X2.3	0,718	0,361	Valid
X2.4	0,702	0,361	Valid
X3.1	0,756	0,361	Valid
X3.2	0,721	0,361	Valid
X3.3	0,688	0,361	Valid
X3.4	0,734	0,361	Valid
X4.1	0,742	0,361	Valid
X4.2	0,769	0,361	Valid

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Item Pernyataan	r hitung	r tabel	Keterangan
X4.3	0,711	0,361	Valid

Berdasarkan hasil pengujian pada Tabel 2, seluruh item pernyataan memiliki nilai r hitung lebih besar dari r tabel, sehingga dapat disimpulkan bahwa seluruh item kuesioner valid dan layak digunakan dalam penelitian.

Hasil Uji Reliabilitas

Uji reliabilitas dilakukan untuk mengukur tingkat konsistensi internal instrumen penelitian. Pengujian reliabilitas menggunakan metode *Cronbach's Alpha* terhadap 15 item pernyataan.

Tabel 3. Reability Statistics

Reliability Statistics

Cronbach's Alpha	N of Items
.882	15

Hasil uji reliabilitas menunjukkan nilai Cronbach's Alpha sebesar 0,882 (>0,70), sehingga instrumen dinyatakan reliabel. Seluruh item memiliki nilai corrected item-total correlation >0,30, sehingga semua item dinyatakan konsisten dan layak digunakan dalam penelitian.

Analisis Deskriptif

Analisis deskriptif digunakan untuk memberikan gambaran umum mengenai tingkat perilaku keamanan informasi pengguna aplikasi Shopee sebelum dilakukan analisis inferensial. Analisis ini bertujuan untuk mengidentifikasi kecenderungan perilaku responden berdasarkan empat dimensi dalam *Security Behavior Intentions Scale (SeBIS),* yaitu *Proactive Awareness*, *Password Generation*, *Software Updating*, dan *Device Securement*.

Tabel 4. Descriptive Statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Proactive Awarness_X1	251	2,50	5,00	4,3466	,56469
Password Generation_X2	251	1,25	5,00	4,2809	,64132
Software Updating_X3	251	1,00	5,00	4,1660	,74974
Device Securement_X4	251	1,00	5,00	3,9960	,83095
Perilaku Keamanan Informasi (Y)	251	23,00	75,00	62,9920	9,16471
Valid N (listwise)	251				

Berdasarkan hasil analisis deskriptif terhadap 251 responden, diperoleh gambaran tingkat perilaku keamanan informasi pengguna aplikasi Shopee yang diukur menggunakan instrumen Security Behavior Intentions Scale (SeBIS). Hasil analisis

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

menunjukkan bahwa dimensi Proactive Awareness (X_1) memiliki nilai rata-rata (mean) tertinggi yaitu sebesar 4,35 dengan simpangan baku sebesar 0,56. Temuan ini menunjukkan bahwa responden memiliki tingkat kesadaran yang tinggi terhadap potensi risiko keamanan informasi saat menggunakan teknologi digital.

Sebaliknya, dimensi Device Securement (X_4) memiliki nilai rata-rata terendah yaitu sebesar 3,99 dengan simpangan baku sebesar 0,83. Meskipun masih berada pada kategori tinggi, nilai ini lebih rendah dibandingkan dimensi lainnya sehingga menunjukkan bahwa aspek pengamanan perangkat merupakan dimensi yang relatif paling lemah dibandingkan dimensi lainnya dalam perilaku keamanan informasi responden.

Dimensi lainnya juga menunjukkan nilai rata-rata yang cukup tinggi. Dimensi Password Generation (X_2) memiliki nilai mean sebesar 4,28 dengan standar deviasi sebesar 0,64, sedangkan dimensi Software Updating (X_3) memiliki nilai mean sebesar 4,17 dengan standar deviasi sebesar 0,75. Secara umum, keempat dimensi tersebut menunjukkan nilai rata-rata di atas 3,50 yang menunjukkan bahwa responden memiliki tingkat perilaku keamanan informasi yang baik.

Berdasarkan nilai rata-rata tersebut, dapat disimpulkan bahwa perilaku keamanan informasi responden cenderung positif. Nilai mean yang mendekati angka 4,00 menunjukkan bahwa mayoritas responden memberikan jawaban setuju terhadap pernyataan dalam instrumen SeBIS. Hal ini mengindikasikan bahwa pengguna aplikasi Shopee dalam penelitian ini telah memiliki tingkat kesadaran dan praktik keamanan informasi yang cukup baik, khususnya dalam aspek kesadaran proaktif terhadap ancaman keamanan serta praktik pembuatan kata sandi yang aman.

Selain itu, nilai simpangan baku pada masing-masing dimensi berada di bawah angka 1,00, yaitu 0,56 pada Proactive Awareness, 0,64 pada Password Generation, 0,75 pada Software Updating, dan 0,83 pada Device Securement. Nilai simpangan baku yang relatif kecil menunjukkan bahwa jawaban responden cenderung homogen atau tidak memiliki perbedaan yang terlalu besar antar responden.

Namun demikian, dimensi Device Securement memiliki nilai simpangan baku paling tinggi dibandingkan dimensi lainnya. Hal ini menunjukkan bahwa terdapat variasi perilaku responden yang lebih besar dalam hal pengamanan perangkat, seperti penggunaan fitur keamanan perangkat atau perlindungan akses pada perangkat yang digunakan.

Korelasi Pearson

Tabel 5. Hasil Uji Korelasi Pearson

Correlations

		Proactive Awarness	Password Generation	Software Updating	Device Securement	Perilaku Keamanan Informasi (Y)
Proactive Awarness _X1	Pearson Correlation	1	,729**	,657**	,667**	,854**
	Sig. (2-tailed)		,000	,000	,000	,000
	N	251	251	251	251	251
	Pearson Correlation	,729**	1	,714**	,714**	,894**

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Password Generation _X2	Sig. (2-tailed)	,000		,000	,000	,000
	N	251	251	251	251	251
Software Updating _X3	Pearson Correlation	,657**	,714**	1	,712**	,865**
	Sig. (2-tailed)	,000	,000		,000	,000
	N	251	251	251	251	251
Device Securement _X4	Pearson Correlation	,667**	,714**	,712**	1	,902**
	Sig. (2-tailed)	,000	,000	,000		,000
	N	251	251	251	251	251
Perilaku Keamanan Informasi (Y)	Pearson Correlation	,854**	,894**	,865**	,902**	1
	Sig. (2-tailed)	,000	,000	,000	,000	
	N	251	251	251	251	251

**. Correlation is significant at the 0.01 level (2-tailed).

Berdasarkan hasil uji korelasi Pearson pada Tabel 5, diperoleh nilai signifikansi (Sig.) pada seluruh variabel lebih kecil dari 0,05 ($p < 0,001$). Hal ini menunjukkan bahwa terdapat hubungan yang signifikan antara masing-masing variabel penelitian dengan perilaku keamanan informasi (Y) pengguna aplikasi Shopee di Kota Bandung.

Seluruh variabel menunjukkan hubungan yang positif dengan perilaku keamanan informasi. Hal ini berarti bahwa semakin tinggi nilai pada masing-masing variabel, maka semakin tinggi pula tingkat perilaku keamanan informasi yang ditunjukkan oleh responden.

Variabel Proactive Awareness (X_1) memiliki koefisien korelasi sebesar 0,854, yang termasuk dalam kategori sangat kuat. Temuan ini menunjukkan bahwa tingkat kesadaran pengguna terhadap potensi risiko keamanan, seperti kewaspadaan terhadap tautan mencurigakan, kehati-hatian dalam membagikan informasi pribadi, serta kesadaran terhadap ancaman keamanan digital, memiliki hubungan yang sangat kuat dengan perilaku keamanan informasi.

Variabel Password Generation (X_2) memiliki koefisien korelasi sebesar 0,894, yang juga termasuk dalam kategori sangat kuat. Hal ini menunjukkan bahwa praktik pembuatan kata sandi yang kuat, unik, dan dikelola dengan baik memiliki hubungan yang sangat kuat dengan perilaku keamanan informasi pengguna.

Variabel Software Updating (X_3) memiliki nilai korelasi sebesar 0,865, yang termasuk dalam kategori sangat kuat. Temuan ini menunjukkan bahwa kebiasaan pengguna dalam melakukan pembaruan perangkat lunak dan aplikasi secara berkala memiliki hubungan yang kuat dengan perilaku keamanan informasi.

Variabel Device Securement (X_4) memiliki nilai korelasi paling tinggi dengan perilaku keamanan informasi, yaitu sebesar 0,902, yang juga termasuk dalam kategori sangat kuat. Hal ini menunjukkan bahwa praktik pengamanan perangkat, seperti penggunaan PIN, kata sandi layar, pola kunci, maupun autentikasi biometrik, memiliki hubungan yang sangat kuat dengan perilaku keamanan informasi pengguna.

Secara keseluruhan, hasil penelitian menunjukkan bahwa keempat variabel penelitian, yaitu Proactive Awareness, Password Generation, Software Updating, dan Device Securement, memiliki hubungan yang kuat dan signifikan dengan perilaku

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno
keamanan informasi pengguna aplikasi Shopee di Kota Bandung. Temuan ini menunjukkan bahwa peningkatan pada aspek kesadaran keamanan, pengelolaan kata sandi, pembaruan perangkat lunak, serta pengamanan perangkat berkaitan dengan peningkatan perilaku keamanan informasi pengguna.

Pembahasan

Penelitian ini bertujuan untuk menganalisis perilaku keamanan informasi pengguna aplikasi Shopee di Kota Bandung menggunakan framework Security Behavior Intentions Scale (SeBIS), serta mengkaji hubungan masing-masing dimensi SeBIS dengan perilaku keamanan informasi (Y). Berdasarkan hasil analisis, diperoleh beberapa temuan penting terkait praktik keamanan digital pengguna e-commerce.

1. Gambaran tingkat perilaku keamanan informasi pengguna Shopee

Hasil analisis deskriptif menunjukkan bahwa perilaku keamanan informasi pengguna Shopee berada pada kategori tinggi. Hal ini terlihat dari nilai rata-rata setiap dimensi SeBIS yang berada di atas 3,50, yang menunjukkan kecenderungan positif dalam penerapan praktik keamanan digital.

Dimensi dengan nilai rata-rata tertinggi adalah Proactive Awareness (X_1), yang menunjukkan bahwa pengguna memiliki tingkat kewaspadaan yang baik terhadap potensi risiko keamanan digital. Sebaliknya, dimensi Device Securement (X_4) memiliki nilai rata-rata paling rendah meskipun masih berada pada kategori tinggi. Hal ini menunjukkan bahwa penerapan pengamanan perangkat seperti penggunaan kunci layar, PIN, atau autentikasi biometrik masih bervariasi di antara responden.

Temuan ini menunjukkan bahwa meskipun tingkat kesadaran keamanan pengguna sudah cukup baik, penerapan praktik teknis dalam pengamanan perangkat masih perlu ditingkatkan.

2. Hubungan dimensi SeBIS dengan perilaku keamanan informasi

Hasil uji korelasi Pearson menunjukkan bahwa seluruh dimensi dalam SeBIS memiliki hubungan positif dan signifikan dengan perilaku keamanan informasi (Y). Hal ini menunjukkan bahwa peningkatan pada masing-masing dimensi berkaitan dengan peningkatan perilaku keamanan informasi pengguna.

Dimensi Device Securement (X_4) menunjukkan hubungan paling kuat dengan perilaku keamanan informasi. Hal ini menunjukkan bahwa praktik pengamanan perangkat seperti penggunaan PIN, kata sandi layar, atau autentikasi tambahan berkaitan erat dengan tingkat perilaku keamanan informasi pengguna.

Dimensi Password Generation (X_2) juga menunjukkan hubungan yang sangat kuat dengan perilaku keamanan informasi. Temuan ini mengindikasikan bahwa praktik pembuatan dan pengelolaan kata sandi yang baik, seperti penggunaan kata sandi yang kuat dan unik, berkaitan dengan perilaku keamanan informasi yang lebih baik.

Selain itu, dimensi Software Updating (X_3) juga memiliki hubungan yang kuat dengan perilaku keamanan informasi. Kebiasaan melakukan pembaruan sistem operasi maupun aplikasi secara berkala dapat membantu meningkatkan keamanan digital pengguna karena pembaruan biasanya mencakup perbaikan kerentanan sistem.

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

Sementara itu, Proactive Awareness (X_1) juga menunjukkan hubungan yang sangat kuat dengan perilaku keamanan informasi. Tingkat kesadaran terhadap potensi ancaman keamanan digital berkaitan dengan kecenderungan pengguna untuk lebih berhati-hati dalam menggunakan layanan digital.

3. Implikasi terhadap praktik keamanan digital masyarakat

Secara umum, hasil penelitian menunjukkan bahwa praktik keamanan digital pengguna Shopee di Kota Bandung berada pada tingkat yang baik. Namun demikian, aspek pengamanan perangkat masih perlu mendapat perhatian lebih karena menunjukkan nilai rata-rata yang relatif lebih rendah dibandingkan dimensi lainnya.

Temuan ini menunjukkan bahwa kesadaran masyarakat terhadap keamanan informasi dalam penggunaan layanan digital sudah cukup baik. Meski demikian, peningkatan konsistensi dalam menerapkan praktik keamanan teknis, seperti pengamanan perangkat dan pembaruan sistem secara berkala, tetap diperlukan untuk memperkuat perlindungan data dan akun pengguna.

4. SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa perilaku keamanan informasi pengguna aplikasi Shopee di Kota Bandung berada pada kategori tinggi. Hal ini menunjukkan bahwa sebagian besar responden telah menerapkan praktik keamanan digital yang baik dalam penggunaan *platform e-commerce*

Hasil analisis menunjukkan bahwa seluruh dimensi dalam *Security Behavior Intentions Scale (SeBIS), yaitu Proactive Awareness (X_1), Password Generation (X_2), Software Updating (X_3), dan Device Securement (X_4),* memiliki hubungan positif dan signifikan dengan perilaku keamanan informasi (Y). Hal ini menunjukkan bahwa semakin tinggi tingkat kesadaran keamanan, praktik pengelolaan kata sandi, kebiasaan memperbarui perangkat lunak, serta pengamanan perangkat, maka semakin baik pula perilaku keamanan informasi pengguna.

Di antara keempat dimensi tersebut, *Device Securement (X_4)* menunjukkan nilai korelasi paling tinggi dengan perilaku keamanan informasi. Temuan ini menunjukkan bahwa praktik pengamanan perangkat, seperti penggunaan PIN, pola kunci, atau autentikasi tambahan, memiliki hubungan yang sangat kuat dengan perilaku keamanan informasi pengguna aplikasi Shopee.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa berbagai dimensi perilaku keamanan dalam kerangka SeBIS berkaitan erat dengan perilaku keamanan informasi pengguna dalam menggunakan layanan e-commerce.

UCAPAN TERIMAKASIH

Ucapan terima kasih disampaikan kepada dosen pembimbing yang telah memberikan arahan, bimbingan, serta dukungan selama proses pelaksanaan penelitian hingga penyusunan manuskrip ini. Penulis juga menyampaikan terima kasih kepada keluarga yang senantiasa memberikan dukungan moral, motivasi, serta doa sehingga penelitian ini dapat diselesaikan dengan baik. Selain itu, penulis secara khusus

Djtechno : Jurnal Teknologi Informasi
Vol. 7, No. 1 April 2026
E-ISSN: 2745-3758, P-ISSN : 2776-8546 DOI: 10.46576/djtechno

mengucapkan terima kasih kepada Kethryn Keflin Rike yang telah memberikan dukungan, semangat, serta kontribusi dalam proses penyelesaian penelitian ini. Dukungan dan motivasi yang diberikan sangat berarti bagi penulis dalam menyelesaikan penelitian dan penulisan manuskrip ini.

REFERENCES

[1]. H. Santoso, B. Nugroho, dan R. Lestari, "Kepercayaan dan Perlindungan Informasi di E-Commerce," *J. Teknol. Inf. dan Bisnis Digital*, vol. 4, no. 1, pp. 12–21, 2020.
[2]. "Southeast Asia E-commerce Market Map 2023," 2023. [Online]. Tersedia: https://momentum.asia
[3]. R. S. Salim, M. Hayu, D. Agustintia, R. Annisa, dan M. Y. I. Daulay, "The Effect of Trust, Perceived Risk and E-Service Quality on the Intention to Purchase of E-Commerce Consumers in Indonesia," *J. Madani Society*, vol. 2, no. 1, pp. 53–66, Apr. 2023. [Online]. Tersedia: https://www.researchgate.net/publication/371320223
[4]. Asmarani dan Usman, "Kepercayaan dan Pengaruhnya terhadap Keputusan Pembelian Online," *J. Teknol. dan Bisnis*, vol. 5, no. 2, pp. 101–110, 2020.
[5]. M. Arief, "Why Customers Buy an Online Product? The Effects of Advertising Attractiveness, Influencer Marketing, and Online Customer Reviews," *Emerald Insight*, vol. 2, no. 1, pp. 45–60, 2021. [Online]. Tersedia: https://www.emerald.com/insight/content/doi/10.1108/lbsjmr-09-2022-0052/full/html
[6]. S. Egelman, M. Harbach, and E. Peer, "Beyond the individual: The role of socio-technical context in security behavior," in *Proc. Symp. Usable Privacy and Security (SOUPS)*, USENIX Association, 2016.
[7]. D. Cannistra, "Digital Convergence and Electronic Commerce: Customs and Trade Implications," *Crowell & Moring LLP*, Dec. 2010. https://www.crowell.com/en/insights/publications/digital-convergence-and-electronic-commerce-customs-and-trade-implications
[8]. P. Ifinedo, "Information security awareness and behavior: A study of the Nigerian banking sector," *J. Inf. Syst. Technol. Manag.*, vol. 9, no. 1, pp. 5–24, 2012. https://www.scielo.br/j/jistm/a/G9wLqM6BxQHFkv6wbKJkPhc/?lang=en
[9]. M. Warkentin, A. C. Johnston, E. Walden, and D. Straub, "A theory of security behavior: An application to information security," *Int. J. Inf. Manag.*, vol. 36, no. 2, pp. 246–256, 2016.
[10]. We Are Social & Meltwater, *Digital 2024: Indonesia*. DataReportal, 2024. https://datareportal.com/reports/digital-2024-indonesia
[11]. Sea Ltd., *Sea Group Annual Report 2023*. Shopee Singapore, 2023. https://sea.com/investor/home
[12]. Badan Pusat Statistik Kota Bandung, *Persentase Penduduk Kota Bandung Berumur 5 Tahun ke Atas yang Mengakses Internet dalam 3 Bulan Terakhir Menurut Jenis Kelamin dan Tujuan Mengakses Internet, 2023*. https://bandungkota.bps.go.id/
[13]. Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D, Bandung: Alfabeta, 2021.
[14]. Badan Siber dan Sandi Negara. (2023). *Laporan Tahunan Keamanan Siber Indonesia 2023*. Jakarta: BSSN.
[15]. Kementerian Komunikasi dan Informatika. (2023). *Survei Literasi Digital Nasional 2023*. Jakarta: Kominfo. DetikInet. (2024, 15 Februari). *Waspada! Banyak Kasus Penipuan Akun Shopee Pay karena Bagi Kode OTP*. https://inet.detik.com/
[16]. CNN Indonesia. (2023, 8 November). *Phishing dan Promo Palsu Shopee Marak, Begini Cara Menghindarinya*. https://www.cnnindonesia.com/ Kaspersky. (2023). *The State of Cybersecurity Behavior in Southeast Asia*. https://www.kaspersky.com/