*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

# PENGUKURAN KEAMANAN PENGGUNA ANDROID MENGGUNAKAN *EXPECTACY BASED MODEL* DAN *ALTERNATIVE THREAT BASED MODEL*

**Dio Febrillian Tanjung[1], Wella[2*]**

[1,2] Sistem Informasi, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara, Tangerang, Indonesia
Email: [1]dio.tanjung@student.umn.ac.id, [2*]wella@umn.ac.id
(* : coressponding author)

**Abstrak-** Saat ini, 132,7 juta smartphone digunakan di Indonesia, menunjukkan bahwa *smartphones* merupakan perangkat penting bagi masyarakat Indonesia. Jumlah pengguna yang terus meningkat setiap tahunnya, dan popularitas smartphone dengan sistem operasi Android menunjukkan bahwa pengguna Android juga rentan terhadap ancaman. Setelah melihat kerentanan ini, dianggap penting untuk melacak tindakan pengguna untuk meningkatkan kesadaran pengguna akan tindakan yang salah. Metode yang digunakan dalam penelitian ini adalah *Expectacy Based Model* dan *Alternative Threat Based Model*. Model pertama memiliki variabel dependen perilaku dan variabel independen seperti *susceptibility, severity, susceptibility x severity, efficacy, cost, trust*, dan *user shopiscation*. Model kedua memiliki variabel dependen perilaku dan variabel independen seperti *malware, data leakage, data theft*, biaya sosial, kepercayaan, dan pengguna perdagangan. Analisis akan dilakukan menggunakan tools SPSS.

**Kata Kunci:** Android, *Alternative Threat Based Model*, *Behavior*, *Expectacy Based Model*, *Smartphone*

**Abstract-** *Currently, the number of smartphone users in Indonesia has reached 132.7 million, indicating that smartphones have become a very important device for Indonesian people. The number of smartphone users will continue to increase every year, and the fact that smartphones with the Android operating system are one of the most popular in the Indonesian market shows that Android users are also vulnerable to danger. After seeing this vulnerability, it is considered important to track user actions to increase user awareness of wrong actions. The methods used in this study are Expectancy Based Model and Alternative Threat Based Model. The first model has a dependent variable of behavior and independent variables such as susceptibility, severity, susceptibility x severity, efficacy, cost, trust, and user shopping. The second model has a dependent variable of behavior and independent variables such as malware, data leakage, data theft, social costs, trust, and user trading. The analysis will be carried out using the SPSS tool.*

***Keywords****: Android, Alternative Threat Based Model, Behavior, Expectacy Based Model, Smartphone*

## 1. PENDAHULUAN

Saat ini, sebanyak 132,7 juta orang di Indonesia menggunakan *smartphone* [1], yang menunjukkan bahwa perangkat ini telah menjadi bagian penting dalam kehidupan masyarakat Indonesia [2]. Jumlah pengguna smartphone diperkirakan akan terus bertambah setiap tahun, dengan perangkat berbasis sistem operasi Android menjadi salah satu yang paling populer. Selain itu, terdapat 9 juta aplikasi yang teridentifikasi sebagai malware, 9 juta aplikasi yang tidak dikenal, 3 juta perangkat Android yang terinfeksi, 1 juta aplikasi dengan ulasan buruk, 37 juta malware terdeteksi dalam enam bulan terakhir, dan hampir 1 juta dari 4 juta alamat yang dianalisis mengandung konten berbahaya [3]. Namun, aplikasi seperti *e-commerce* memiliki platform yang kuat karena kekuatan pengolahan yang tangguh dan ramah lingkungan pengembang aplikasi [4]. Kelemahan mungkin terletak pada keamanan *smartphone*. Pengguna *smartphone* sering melakukan kesalahan kecil dalam menjaga data [5]. Sangat penting untuk memperhatikan kecenderungan untuk memasang aplikasi pihak ketiga tanpa melakukan pemeriksaan menyeluruh [11]. *Smartphone* sangat mengancam keamanan data. Ini karena sering digunakan di jaringan umum yang tidak aman seperti bandara dan kedai kopi, dan dapat hilang secara fisik [6]. *Smartphone* adalah perangkat "sosial", sehingga *malware* dapat menyebar dengan cepat. Pengguna telah menjadi "target virus, worms, dan program *malware* lainnya" karena peningkatan kekuatan prosesor dan penyebaran perangkat mobile, seperti yang diantisipasi sepuluh tahun sebelumnya. Data di atas juga menunjukkan bahwa tingkat serangan yang terjadi di Indonesia sangat tinggi, yang harus menjadi perhatian publik Indonesia, terutama bagi pengguna Android. Dengan banyaknya pengguna Android di Indonesia, pengujian keamanan pengguna Android harus dilakukan melalui kebiasaan pengguna. Namun, usia pengguna internet di Indonesia terdiri dari 10–24 tahun, 75.5%, 25–34 tahun, 76.1%, dan 35–44 tahun. Menurut data, penelitian ini terfokus pada 3 siswa S-1 (Strata-1) dalam rentang usia 18-25 tahun, yang dikenal sebagai dewasa dini. Kemampuan mental mencapai puncaknya pada usia 20 tahun, ketika pengguna mulai beradaptasi dengan situasi baru seperti berfikir kreatif, penalaran analogis, dan mengingat apa yang telah dipelajari [7]. Dengan harapan bahwa kebiasaan pengguna terhadap keamanan pengguna tersebut dapat dipengaruhi oleh usia 18 hingga 25 tahun, fokus penelitian ini dipilih

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

untuk usia ini. Penelitian ini bermanfaat secara akademis dengan memberikan wawasan tentang perilaku keamanan pengguna muda smartphone di Indonesia, yang dapat menjadi dasar untuk penelitian lanjutan. Secara praktis, temuan ini membantu pengembang aplikasi dan regulator dalam merancang fitur atau kebijakan keamanan yang lebih sesuai untuk pengguna usia 18-25 tahun. Selain itu, penelitian ini berkontribusi pada peningkatan kesadaran keamanan digital di masyarakat.

Penelitian terdahulu berfokus pada perilaku pengguna dalam konteks keamanan informasi, dengan penekanan pada faktor-faktor yang memengaruhi kepatuhan terhadap kebijakan keamanan, kerentanannya terhadap ancaman, serta tantangan yang dihadapi dalam manajemen risiko dan kebijakan keamanan. Meskipun masing-masing artikel memiliki pendekatan yang berbeda — baik dari perspektif psikologis, kultural, maupun praktis — mereka saling melengkapi dalam memberikan pemahaman yang lebih holistik tentang bagaimana individu dan organisasi mengelola risiko di dunia digital. Salah satu tema utama yang menghubungkan artikel-artikel ini adalah pentingnya faktor psikologis dan perilaku individu dalam keamanan informasi. Dalam konteks perilaku keamanan pribadi, tentang perilaku keamanan smartphone, mengkaji keamanan perangkat di India, menunjukkan bahwa pengetahuan dan persepsi individu terhadap risiko berperan besar dalam menentukan apakah mereka akan mengambil langkah-langkah pengamanan yang diperlukan [8], [9]. Misalnya, sikap terhadap ancaman dan tingkat kepercayaan diri dalam teknologi menjadi faktor kunci dalam keputusan untuk mengadopsi langkah-langkah pengamanan seperti penguncian layar dan pembaruan perangkat [8]. Meskipun banyak pengguna smartphone di India menyadari adanya ancaman, kurangnya pelatihan dan pemahaman mendalam tentang phishing mengurangi efektivitas mereka dalam melindungi perangkat dari ancaman tersebut [9].

Selain itu, pendidikan dan pelatihan menjadi aspek yang saling terkait, terdapat penekanan pada pentingnya edukasi untuk meningkatkan kesadaran keamanan dan pemahaman tentang risiko [8], [9]. Penelitian ini mencatat bahwa kesadaran dan pengetahuan yang lebih baik dapat mengurangi kerentanannya terhadap serangan siber, seperti serangan spear phishing dan pengabaian praktik keamanan dasar. Pendidikan yang efektif bisa memperkuat kontrol perilaku yang dirasakan, sebuah faktor yang juga penting di mana pelatihan dan kebijakan yang jelas dapat mempengaruhi sikap, norma subjektif, dan kontrol perilaku yang dirasakan, yang semuanya berkontribusi pada kepatuhan terhadap kebijakan keamanan informasi.

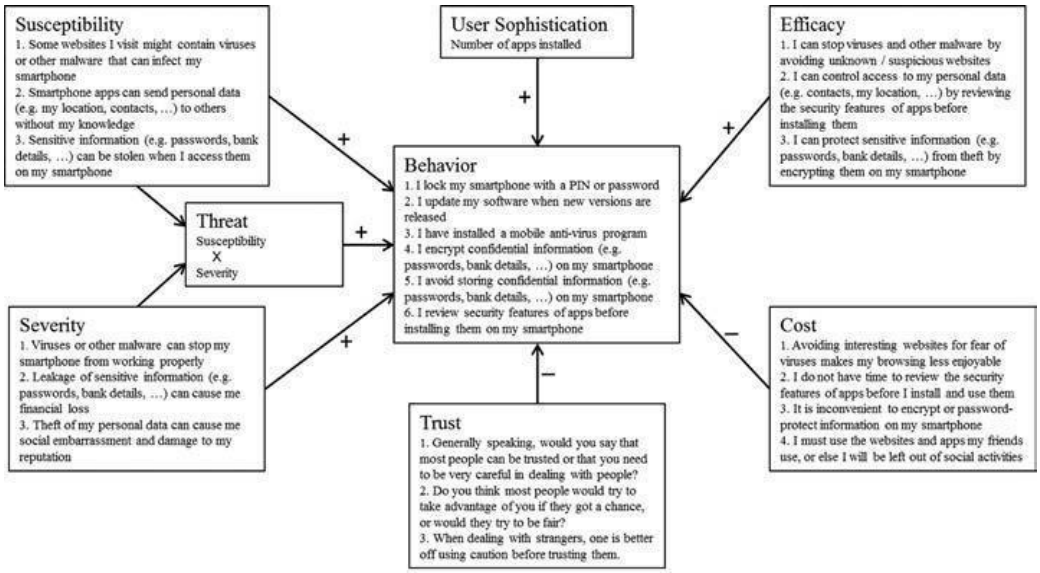
Model TPB yang digunakan dalam penelitian ini memberikan wawasan penting tentang bagaimana sikap, norma sosial, dan kontrol perilaku yang dirasakan berkontribusi terhadap niat dan tindakan individu dalam mematuhi kebijakan tersebut. Pendekatan ini lebih psikologis dan berfokus pada kebijakan dan sikap karyawan dalam organisasi. Di sisi lain, menyoroti kerentanannya terhadap serangan siber di komunitas non-Inggris, khususnya dalam konteks spear phishing. Mereka menyoroti pentingnya faktor kultural dan bahasa dalam meningkatkan kerentanannya terhadap serangan siber. Penelitian ini mengungkapkan bahwa faktor budaya dan kebiasaan komunikasi yang tinggi dalam masyarakat non-Inggris dapat membuat serangan phishing yang disesuaikan dengan bahasa lokal lebih efektif dan sulit dikenali [10].

Bisa dilihat dari beberapa artikel di atas bahwa ada persamaan dan perbedaan antara penelitian ini dan penelitian sebelumnya. Persamaan dari penelitian ini terhadap penelitian sebelumnya adalah penggunaan model berbasis ancaman alternatif yang juga digunakan dalam penelitian ini dan pengamatan kebiasaan pengguna dapat mempengaruhi keamanan pengguna. Perbedaan dari penelitian ini terhadap penelitian sebelumnya adalah lokasi penelitian di Indonesia.

## 2. METODE PENELITIAN

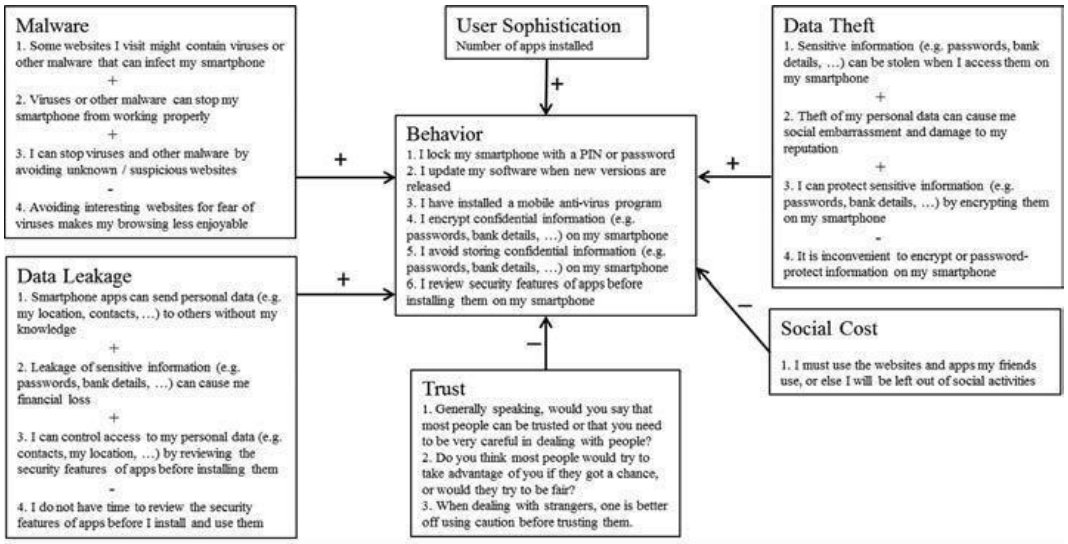
Gambar 1 menunjukkan model expectancy-based model yang disusun ulang untuk memenuhi tujuan penelitian. Variabel pertanyaan didasarkan pada ancaman-ancaman yang berfokus pada masalah keamanan smartphone, dan model kedua didasarkan pada expectancy-based model yang disusun ulang variabelnya untuk dijadikan perbandingan dalam penelitian ini. Dalam model pertama, perilaku didasarkan pada ancaman seperti kepekaan, kekerasan, dan efektivitas, sedangkan dalam model kedua, perilaku didasarkan pada serangan langsung seperti malware, kehilangan data, dan penipuan. Variabel kepercayaan tetap dimasukkan ke kedua model dan tidak berubah

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index




**Gambar 1.** *Expectancy-based model and operationalization*

Kemudian, untuk model pertama, variabel biaya dan biaya sosial diubah. Biaya disusun berdasarkan biaya yang harus dibayar ketika menghindari ancaman dan biaya yang terjadi ketika ancaman terjadi. Dalam penelitian sebelumnya, kedua model ini digunakan untuk membandingkan masing-masing perilaku dari perspektif yang berbeda. Penelitian sebelumnya bertujuan untuk mengetahui apakah pengguna cenderung memperhatikan perilaku pengguna terhadap ancaman-ancaman dan biaya yang dirasakan pada model pertama. Kemudian, kuesioner model kedua dibentuk ulang untuk melihat bagaimana tiga ancaman malware, data leakage, dan data theft berdampak pada perilaku pengguna.




**Gambar 2.** *Alternative Threat Based Model*

## 2.1 Objek Penelitian

Tujuan dari penelitian ini adalah untuk mengetahui bagaimana pengguna Android menangani keamanan perangkat dan mengukur bagaimana respons mencegah atau melindungi data atau informasi penting. Untuk mencapai tujuan ini, survei akan dibagikan secara acak kepada peserta berusia 18 hingga 25 tahun. Karena populasi terbesar pengguna internet pada tahun 2017 adalah kelompok usia 18-34 tahun, dengan presentase 49,52%, diikuti oleh populasi pengguna smartphone sebesar 50,08%, populasi pengguna internet dengan tingkat pendidikan S-1 sebesar 79,23%, dan populasi pengguna internet dengan tingkat pendidikan SMA sebesar 70,54% [12]. Oleh karena itu, kelompok umur 18-25 tahun dianggap cukup sebagai contoh objek untuk penelitian ini [12]. Penelitian ini melibatkan

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

semua responden yang memiliki *smartphone* Android. Sampel dalam penelitian ini berumur 18 hingga 25 tahun. Sampel awal sebanyak 200 orang dihitung dengan menggunakan rumus perhitungan jumlah sampel tergantung pada jumlah indikator, yang dalam penelitian ini adalah dikali 5 [13]. Indikator penelitian terdiri dari 31 dengan 5 variabel, sebagai berikut:

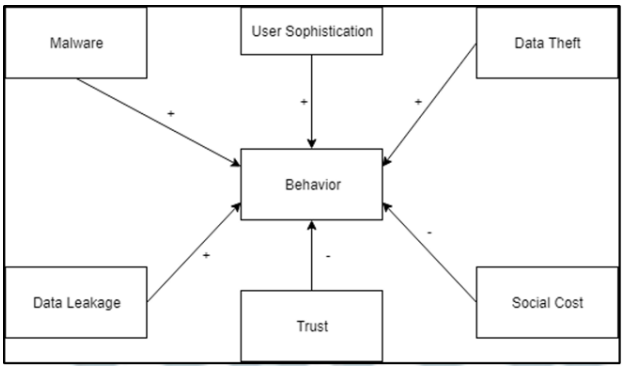
$$\text{Sampel minimum} = 31 \times 5 = 155 \text{ Responden} \quad (1)$$

Berdasarkan perhitungan sebelumnya, jumlah sampel minimum yang diperlukan dalam penelitian ini adalah 155 responden. Namun, untuk meminimalkan risiko kesalahan, penelitian ini akan menggunakan 200 responden sebagai sampel.

## 2.2 Metode Penelitian

Metode penelitian terdahulu menggunakan model Expectacy Based sebagai alat pengukuran perilaku pengguna Android. Model ini dibangun dengan penilaian ancaman yang ada. Setidaknya tiga kelompok ancaman keamanan smartphone telah ditemukan [14]:

1. *Malware*, adalah perangkat lunak yang dirancang untuk merusak, mengganggu, mencuri data, atau mendapatkan akses tidak sah ke sistem komputer. *Malware* mencakup berbagai jenis ancaman, seperti *virus*, *worm*, *spyware*, *trojan horse*, *ransomware*, dan *adware*.
2. *Data Leakage*: kejadian di mana data sensitif atau rahasia secara tidak sengaja atau dengan sengaja terungkap kepada pihak yang tidak berwenang. Data ini dapat mencakup informasi pribadi (seperti nama, alamat, dan data keuangan), data perusahaan, atau data rahasia lainnya. *Data leakage* sering kali terjadi akibat kelemahan teknis, kesalahan manusia, atau serangan siber.
3. *Data Theft*: tindakan mengambil data yang bersifat pribadi, rahasia, atau sensitif tanpa izin pemiliknya. Data yang dicuri dapat berupa informasi pribadi (seperti nomor identitas, data finansial, atau kata sandi), data perusahaan (seperti rahasia dagang), atau data lain yang memiliki nilai bagi penyerang.




**Gambar 3.** Expectacy-Based Model

Dalam model yang ditunjukkan pada Gambar 3, kerentanan terhadap masalah keamanan diukur melalui tiga aspek: *data theft*, *malware*, dan *data leakage*. Adapun dengan tingkat kerentanan, yang meliputi satu indikator untuk setiap potensi kerusakan yang dapat ditimbulkan oleh *data leakage*, *malware*, dan *data theft*. Model ini sering disebut sebagai "kerentanan" karena berpengaruh pada perilaku keamanan. Salah satu dari tiga faktor yang memengaruhi respons terhadap efektivitas adalah sejauh mana tindakan pengamanan dianggap efektif dalam menangani *malware*, *data leakage*, dan *data theft*. Selain itu, model ini mencakup faktor keempat, yaitu ketidaknyamanan, keterbatasan, waktu, serta biaya yang diperlukan untuk melindungi perangkat dari ancaman tersebut, yang sering kali tidak diadopsi oleh masyarakat [11].

Kecanggihan / kemampuan pengguna untuk melindungi diri terhadap ancaman keamanan dikenal sebagai self-*efficacy*. menggunakan sejumlah aplikasi yang terinstal di ponsel pintar pengguna sebagai proxy untuk transaksi pengguna dalam penelitian ini. Hal ini bertujuan dengan harapan "Pengguna Power" memasang aplikasi lebih banyak daripada pengguna pemula lainnya. Daftar Keamanan Perangkat Lunak Microsoft mengubah ukuran variabel dependen dan perilaku keamanan [11]. Adapun kebiasaan baik yang dilakukan pengguna seperti menyimpan kata sandi dengan baik, melakukan *software update*, melakukan instalasi *anti-virus*, *encryption*, menghindari penyimpanan data pribadi, dan meninjau fitur keamanan aplikasi sebelum menginstalnya adalah dasar dari pertanyaan yang dibuat. Skornya berkorelasi positif dengan jumlah perilaku keamanan yang dilakukan. Kepercayaan, yang bertujuan untuk membangun dan mempertahankan kepercayaan, sangat penting untuk keamanan informasi. Tugas kepercayaan ini harus dijelaskan dengan jelas dan tidak ambigu. Untuk tiga item ukuran kepercayaan, Survey Umum Sosial Amerika dan Kuesioner Panel Sosial Ekonomi Jerman adalah sumbernya. Karena cenderung tidak diganggu oleh orang lain, pengguna *smartphone* yang percaya menunjukkan memiliki tingkat keamanan yang lebih rendah. Dalam penelitian

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

sebelumnya, model I (*Expectacy Based Model*) dimodelkan ulang menjadi model alternatif yang disebut *Expectacy Based Model*—juga dikenal sebagai model II—untuk mengukur bagaimana ketiga ancaman tersebut berkontribusi secara relatif, yaitu *malware*, pencurian data, dan leakage data. Model ini juga disesuaikan untuk kuesioner sebelumnya.

## 2.3 Teknik Pengumpulan Data

Penelitian ini menggunakan metode kuesioner untuk pengumpulan data, dengan sampel sebanyak 200 responden berusia 18 hingga 25 tahun yang tersebar di berbagai kota, seperti Malang, Palangka Raya, Bandung, Solo, Yogyakarta, Jakarta, Semarang, dan Tangerang. Data dikumpulkan menggunakan skala Likert dengan 5 tingkat penilaian, mulai dari sangat tidak setuju hingga sangat setuju. Pertanyaan-pertanyaan tersebut dirancang untuk mengukur pengetahuan pengguna tentang ancaman yang ada, termasuk kesadaran terhadap ancaman, risiko, dan biaya yang terkait [11].

## 2.4 Teknik Analisis Data

Analisis data berganda (multiple regression) akan digunakan. Perilaku adalah variabel kriteria (DV), dan variabel prediktor (IV) adalah kecerdasan pengguna, malware, kehilangan data, pencurian data, biaya sosial, dan kepercayaan. Metode multiple regression (regresi linier berganda) digunakan dalam penelitian ini karena menggunakan lebih dari satu variabel bebas. Setelah hasil perhitungan multiple regression ditemukan, hasilnya akan diperiksa untuk memastikan bahwa mereka sesuai dengan hipotesa.

$$Y' = a + b1X1 + b2X2 + \ldots + bnXn \quad (2)[15]$$

Keterangan:

| | | |
|---|---|---|
| Y’ | : | Variabel dependen (nilai yang diprediksi) |
| X1 dan X2 | : | Variabel independen |
| a | : | Konstanta (nilai Y’ apabila X1, X2,…, Xn = 0) |
| b | : | Koefisien regresi (nilai peningkatan ataupun penurunan) |

Selanjutnya, alat pengolahan data yang digunakan adalah SPSS. Ada beberapa alat pengolahan data lainnya, seperti Microsoft Excel, tetapi Excel memiliki beberapa fungsi yang terbatas, jadi SPSS lebih cocok untuk penelitian ini.

## 2.5 Hipotesis Penelitian

Untuk penelitian ini, hipotesis H1 akan dibuat, yang menunjukkan bahwa untuk setiap model, pengaruh atau penerimaan antara variabel independen dan variabel dependen terjadi dengan signifikansi 5%. Variabel-variabel dari masing-masing model akan dijelaskan sebagai berikut.

Konsumen Toko: Konsumen toko, juga dikenal sebagai kecanggihan pengguna, adalah salah satu variabel yang akan diukur. Studi sebelumnya menunjukkan bahwa tingkat konsumsi toko yang lebih tinggi diharapkan menghasilkan pemahaman pengguna tentang penggunaan teknologi yang lebih baik [11]. Oleh karena itu, hipotesis yang akan diajukan tentang konsumen toko adalah sebagai berikut.

H1 = *User shopiscation* berpengaruh signifikasi positif terhadap *behavior*.

*Susceptibility* adalah variabel yang akan diukur. Banyak penelitian sebelumnya yang membahas mengenai perilaku keamanan secara tidak langsung atau langsung memilih fokus pada ekspektasi, di mana kecenderungan yang dan efektivitas dikombinasikan untuk mendorong proses penilaian ancaman yang melengkapi penilaian perilaku keamanan. Pengguna mungkin lebih baik bertindak jika mereka tahu tentang ancaman yang dapat menyebabkan masalah [11]. Akibatnya, hipotesis variabel ketakutan dapat disusun seperti berikut:

H1 = *Susceptibility* berpengaruh signifikasi positif terhadap *behavior*

*Severity*. Studi sebelumnya menunjukkan bahwa sensitivitas yang dirasakan, intensitas yang dirasakan, efektivitas, dan respons biaya memengaruhi keinginan untuk menggunakan perangkat lunak anti-spyware sebagai teknologi pelindung. Menurut penelitian lain, intensitas pengaruh dari penelitian sebelumnya dapat dibentuk menjadi hipotesa berikut:

H1 = *Severity* berpengaruh signifikasi positif terhadap *behavior*

*Susceptibility* x *Severity*. Seperti yang ditunjukkan oleh penelitian sebelumnya tentang gangguan keamanan dalam organisasi, tingkat ketakutan dan intensitas yang dirasakan, serta tingkat keefektifan dan respons yang tinggi, menurunkan kemungkinan kelalaian yang mengancam keamanan. Dengan dampak ini, hipotesis berikut dapat diperkuat: Variabel *Susceptibility* x *Severity*

H1 = *Susceptibility x Severity* berpengaruh signifikasi positif terhadap *behavior*

*Efficacy*. Studi tentang niat pengguna untuk menggunakan anti-spyware menemukan bahwa persepsi keberhasilan keamanan dan tanggapan *self-efficacy* pengguna dalam melakukan tindakan dipengaruhi secara langsung oleh respons keberhasilan, *self-efficacy*, dan norma sosial, tetapi tidak dengan kerentanan atau tingkat keparahan

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

ancaman yang digambarkan dalam ketakutan banding. Berdasarkan penelitian sebelumnya, hipotesis tentang variabel *efficacy* berikut dapat dibuat:

H1 = *Efficacy* berpengaruh signifikasi positif terhadap *behavior*

*Cost*: Studi terdahulu membuat dan menguji model penghindaran ancaman teknologi dan menemukan bahwa ancaman yang dirasakan (*susceptibility* dan *severity*), keefektifan, dan biaya memengaruhi keinginan untuk menghindari *spyware*. Untuk menghitung variabel biaya, hipotesis berikut dapat digunakan:

H1 = *Cost* berpengaruh signifikasi negatif terhadap *behavior*

*Trust*. Dengan variabel kepercayaan, penelitian sebelumnya menemukan bahwa informasi tentang kebijakan keamanan meningkatkan niat dan perilaku pengguna [30]. Penelitian ini memungkinkan pembuatan hipotesis berikut:

H1 = *Trust* berpengaruh signifikasi negatif terhadap *behavior*

*Data leakage*, *malware*, dan *data theft*: Studi sebelumnya menunjukkan bahwa eksekutif bisnis kecil dan menengah menggunakan perangkat lunak *anti-malware*. telah menemukan bahwa keinginan untuk menggunakan perangkat lunak *anti-malware* dipengaruhi oleh severity yang dirasakan, susceptibility yang dirasakan, efektivitas, biaya sosial, dukungan vendor, dan anggaran TI. Selain itu, ada korelasi positif antara niat yang diungkapkan dan perilaku pemakaian yang sebenarnya. Tiga variabel digunakan dalam pertanyaan-pertanyaan tentang kepekaan terhadap masalah keamanan: satu untuk *malware*, satu lagi untuk data leakage, dan yang ketiga untuk *data theft*. Hal yang sama berlaku untuk tingkat keparahan, dengan satu variabel terdiri dari dampak kerusakan yang dirasakan dari *data theft*, *malware*, dan *data leakage* [11]. Berdasarkan penelitian di atas, hipotesis dapat dibuat yang menggambarkan masing-masing variabel seperti yang ditunjukkan dalam Tabel 4, atau lebih lanjut.

H1 = *Malware* berpengaruh signifikasi positif terhadap *behavior*

H1 = *Data leakage* berpengaruh signifikasi positif terhadap *behavior*

H1 = *Data theft* berpengaruh signifikasi positif terhadap *behavior*

Sosial *Cost*. Selain itu, biaya termasuk hal keempat: kehilangan kenyamanan, kemampuan, dan waktu yang dihabiskan untuk melindungi smartphone atau aplikasi populer dari malware, data leakage, dan data theft. Biaya ini mengacu pada biaya sosial yang tidak digunakan dari fitur smartphone atau aplikasi populer: kemungkinan tertinggal dari percakapan, diskusi, dan aktivitas media sosial [11]. Berikut adalah hasil penelitian sebelumnya:

H1= *Social cost* berpengaruh signifikasi negatif terhadap *behavior*

Penjelasan dari tiap variabel di atas akan disusun ke dalam model, pada model I (*Expectacy Based Model*) Tabel 1:

**Tabel 1.** Hipotesis model I

| Deskripsi | |
|---|---|
| H1 | User Sophicisation berdampak positif terhadap *behavior* |
| H2 | *Susceptibilty* berdampak positif terhadap *behavior* |
| H3 | *Severity* berdampak positif terhadap *behavior* |
| H4 | *Susceptibility* x *Severity* berdampak positif terhadap *behavior* |
| H5 | *Efficacy* berdampak positif terhadap *behavior* |
| H6 | *Cost* berdampak negatif terhadap *behavior* |
| H7 | *Trust* berdampak negatif terhadap *behavior* |

Hipotesis model 1 sama dengan model II, di mana variabel independen dipengaruhi atau diterima oleh variabel dependen. Dalam model ini, masing-masing variabel disusun ulang untuk melihat dampak dari ancaman saat ini, yang dapat dilihat pada Tabel 2.

**Tabel 2.** Hipotesis model II

| Deskripsi | |
|---|---|
| H1 | User Sophicisation berdampak positif terhadap *behavior* |
| H2 | *Malware* berdampak positif terhadap *behavior* |
| H3 | *Data leakage* berdampak positif terhadap *behavior* |
| H4 | *Data theft* berdampak positif terhadap *behavior* |
| H5 | *Social cost* berdampak negatif terhadap *behavior* |
| H6 | *Trust* berdampak negatif terhadap *behavior* |

# 3. HASIL DAN PEMBAHASAN

## 3.1 Demografi

Setiap responden dikelompokkan berdasarkan umur dan kota asal. Dari 198 orang yang menjawab, dianggap perlu untuk mengetahui presentasi umur dari sample penelitian. Jumlah responden berumur 18 tahun adalah 7 orang, yang menunjukkan presentasi 3%; berumur 19 tahun adalah 21 orang, yang menunjukkan presentasi 11%; berumur 20 tahun adalah 32 orang, yang menunjukkan presentasi 16.2%; berumur 21 tahun adalah 53 orang, yang menunjukkan presentasi 27%; berumur 22 tahun adalah 47 orang, yang menunjukkan presentasi 24%; berumur 23 tahun adalah 26

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

orang, yang menunjukkan presentasi 13%; dan berumur 24 tahun adalah 8 orang, yang menunjukkan presentasi 4%. Penelitian ini memiliki data yang tidak seimbang antara laki-laki dan perempuan, jadi rata-rata responden berjenis kelamin laki-laki, dengan 125 orang yang berpartisipasi dengan presentasi sebesar 63% dan 73 orang yang berpartisipasi dengan presentasi sebesar 37%. Namun, jenis kelamin hanya digunakan sebagai pemetaan data dan tidak digunakan sebagai tolak ukur untuk menghasilkan hasil akhir. Kota Tangerang Selatan adalah kota yang paling banyak menerima kuesioner, dengan jumlah responden sebanyak 78 orang atau sekitar 39,9%. Kota Palangka Raya mengikuti dengan 32 orang atau sekitar 16%, kota Jakarta dengan 19 orang atau sekitar 9,5%, kota Solo dengan 19 orang atau sekitar 9,5%, Yogyakarta dan Malang dengan 14 orang masing-masing.

## 3.2 Uji Validitas dan Reliabilitas

Setelah kuesioner dibagikan, 214 orang yang menjawab tersebar di kota-kota yang telah ditentukan sebelumnya; 198 dari responden memberikan tanggapan yang valid, dan 16 tanggapan kosong tidak digunakan. Pada penelitian ini, pengujian validitas dilakukan dengan menggunakan korelasi bivariat product moment. Ini digunakan untuk mengetahui seberapa besar korelasi yang dihasilkan dari setiap pertanyaan pada masing-masing indikator. Hasil uji validitas yang dilakukan pada model 1 (*Expectacy Based Model*) dan model 2 (*Alternative Threat Based Model*), yang melibatkan 198 peserta. Pada model 1 (didasarkan pada harapan), semua pertanyaan yang menunjukkan masing-masing indikator dianggap valid karena nilai korelasinya >0,1395 (lihat tabel r di lampiran), dengan nilai signifikasi 0,05, dan tingkat kebebasan (n-2) dengan jumlah data 198 - 2 = 196. Setelah model 1 diuji validitasnya, model 2 juga harus diuji. Menurut Tabel 8, masing-masing pertanyaan yang dikonstruksikan ulang dinyatakan valid, dan pertanyaan P25 dan P31 menerima nilai satu karena hanya ada satu pertanyaan untuk indikator biaya sosial dan toko pengguna.

Pada tahap ini, setelah validitas dinyatakan, masing-masing indikator akan dievaluasi untuk mengetahui apakah kedua model ini cukup akurat untuk digunakan sebagai alat ukur. Nilai alpha model 1 dalam aplikasi perhitungan reliabilitas spss ditemukan yang ditampilkan pada Gambar 4.

**Reliability Statistics**

| Cronbach's Alpha | N of Items |
|---|---|
| ,787 | 31 |

**Gambar 4.** Uji reliabilitas model I

Cronbach's Alpha merupakan sebuah ukuran keandalan yang memiliki nilai berkisa dari nol sampai satu [13]. Nilai tingkat keandalan Cronbach's Alpha minimum adalah 0,70 [13]. Model pertama memiliki nilai Cronbach's Alpha sebesar 0,787, yang menunjukkan bahwa model ini termasuk dalam kategori keandalan yang andal. Oleh karena itu, kedua model ini telah diuji validitas dan reliabilitasnya secara bersamaan (Gambar 5).

**Reliability Statistics**

| Cronbach's Alpha | N of Items |
|---|---|
| ,779 | 31 |

**Gambar 5.** Uji reliabilitas model II

## 3.3 Uji Hipotesis

Berikut adalah analisis lebih lanjut pada setiap hipotesis yang telah ditentukan sebelumnya dengan signifikasi 0.05 nilai t-tabel 1.65356, jika nilai t > 1.65356 maka hipotesis diterima begitu pula sebaliknya jika nilai dari t < 1.65356 maka hipotesis akan ditolak atau data tidak dianggap cukup untuk menjawab hipotesis tersebut.

**Tabel 3.** Analisis Hipotesis Model 1 *Expectacy Based Model*

| Hipotesis | Hubungan | Nilai t | Kesimpulan |
|---|---|---|---|
| H1 | *User shopiscation > Behavior* | 0.329 | Data tidak mendukung H1 |
| H2 | *Susceptibility > Behavior* | 0.103 | Data tidak mendukung H2 |
| H3 | *Severity > Behavior* | 0.821 | Data tidak mendukung H3 |
| H4 | *Susceptibility* x *Severity > Behavior* | -0.071 | Data tidak mendukung H4 |
| H5 | *Efficacy > Behavior* | 2.078 | Data mendukung H5 |
| H6 | *Cost > Behavior* | 0.367 | Data tidak mendukung H6 |
| H7 | *Trust > Behavior* | 1.699 | Data tidak mendukung H7 |

Perhatikan Tabel 3 ditemukan bahwa dari tujuh variabel yang digunakan sebagai prediktor hanya variabel *efficacy* yang memenuhi sebagai prediktor dari *behavior* sedangkan variabel-variabel lain seperti *user shopiscation, susceptibility, severity, susceptibility x severity cost* dan *trust* tidak memenuhi sebagai prediktor *behavior* karena nilai

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

t pada masing-masing variabel tidak melebihi 1.65356, dengan demikian maka pada model I yaitu *Expectacy Based Model* tidak dapat memenuhi hipotesis secara keseluruhan dan hanya satu hipotesis yang diterima.

**Tabel 4.** Analisis Hipotesis Model 2 *Alternative Threat Based Model*

| Hipotesis | Hubungan | Nilai t | Kesimpulan |
|---|---|---|---|
| H1 | *User shopiscation > Behavior* | 0.890 | Data tidak mendukung H1 |
| H2 | *Malware > Behavior* | 3.961 | Data mendukung H2 |
| H3 | *Data leakage > Behavior* | -0.299 | Data tidak mendukung H3 |
| H4 | *Data theft > Behavior* | 1.470 | Data tidak mendukung H4 |
| H5 | *Cost > Behavior* | 0.629 | Data tidak mendukung H5 |
| H6 | *Trust > Behavior* | 2.302 | Data tidak mendukung H6 |

Model II juga akan dilakukan uji hipotesis terlihat pada Tabel 4 bahwa hanya satu variabel saja yaitu *malware* yang memenuhi nilai tabel t dan dianggap valid sebagai prediktor dari *behavior* kemudian untuk variabel-variabel lain seperti *data leakage, data theft, cost* dan *trust* tidak dapat dijadikan variabel perdiktor terhadap *behavior* dikarenakan nilai t pada masing-masing variabel tidak memenuhi nilai pada tabel t, sehingga pada model kedua hanya satu hipotesis saja yang diterima yaitu hipotesis untuk *malware* sedangkan variabel lain hipotesis ditolak.

### 3.4 Hasil Diskusi

Penelitian ini menemukan bahwa masing-masing model baik model I maupun model II tidak dapat dijadikan sebagai model prediktor dalam mengukur keamanan pengguna android melalui kebiasaan pengguna, hal ini terjadi dikarenakan kedua model ini tidak memenuhi koefisien determinasi yang cukup sehingga kedua model ini dianggap tidak dapat digunakan untuk mengukur perilaku pengguna terhadap keamanan secara umum, melihat hasil temuan yang di dapat bahwa masing-masing variabel yang dijadikan prediktor baik pada model 1 yaitu : *susceptibility*, *severity*, *efficacy*, *susceptibility x severity*, *cost*, dan *trust* hanya satu variabel saja yang memenuhi syarat sebagai prediktor dari *behavior* yaitu variabel *efficacy*, sedangkan variabel-variabel lainnya tidak dapat dijadikan prediktor dalam mengukur *behavior*, sehingga model I tidak dapat terpenuhi secara keseluruhan, kemudian untuk model II variabel yang memenuhi syarat hanya *malware* sedangkan variabel lain seperti *data leakage*, *data theft*, *social cost*, dan *trust* tidak memenuhi sebagai prediktor *behavior*. Penelitian ini tidak memenuhi model secara keseluruhan berdasarkan perhitungan regresi berganda namun berhasil menemukan temuan bahwa pengguna *smartphone* merasa bahwa *severity* dan *efficacy* pada model I sebagai hal yang perlu diperhatikan, kemudian pada model II *malware*, *data leakage*, dan *data theft* pengguna beranggapan sebagai ancaman yang harus diperhatikan. Studi sebelumnya menunjukkan bahwa pada model I—yang didasarkan pada harapan—variabel kecenderungan dan intensitas memengaruhi perilaku pengguna OS blackberry secara signifikan, sedangkan variabel kecenderungan x intensitas tidak memengaruhi perilaku. Selanjutnya, untuk efektivitas dan biaya, variabel kecenderungan memengaruhi perilaku secara signifikan positif, sedangkan variabel biaya memengaruhi perilaku secara signifikan negatif untuk semua jensi. Mungkin ada alasan mengapa hasil penelitian ini berbeda dari penelitian sebelumnya karena faktor demografis. Menurut hasil penelitian yang mengangkat perilaku, faktor demografis dapat memengaruhi perilaku. Oleh karena itu, faktor demografis dapat menjadi masalah dalam penelitian ini. Selain itu, metode observasi dapat digunakan sebagai metode pengambilan data; penelitian terdahulu yang mengukur kenyamanan pengguna terhadap keamanan dan privasi menemukan bahwa dengan melihat secara langsung setiap orang, kita dapat memberikan rekomendasi yang tepat tentang cara terbaik untuk melindungi *smartphone*. Oleh karena itu, metode observasi juga dapat digunakan dalam penelitian ini untuk melihat perilaku pengguna secara menyeluruh untuk setiap individu, meskipun metode yang digunakan tidak sesuai dengan perilaku yang diharapkan. Penelitian ini dapat disebut sebagai penelitian tahap awal karena diperlukan perbaikan seperti penambahan atau penggunaan variabel lain seperti pengetahuan. Penelitian tentang pengaruh pengetahuan terhadap konsistensi perilaku menemukan bahwa sikap berdasarkan pengetahuan yang relevan memprediksi perilaku lebih baik daripada sikap berdasarkan pengetahuan yang relevan rendah, terutama dalam kasus di mana orang memiliki waktu yang cukup untuk berunding. Ini harus dibuat mengingat tingkat kesadaran pengguna terhadap bahaya dan bagaimana kebiasaan penggunaan *smartphone* dapat memengaruhi.

## 4. KESIMPULAN

Penelitian ini menemukan bahwa hanya ada dua variabel penting yang digunakan untuk mengukur perilaku pengguna *smartphone*: efektifitas sebagai tindakan dan *malware* sebagai ancaman. Variabel lain yang didasarkan pada ekspektasi, seperti *susceptibility*, *severity*, *susceptibility x severity*, *cost*, kepercayaan, dan transaksi pengguna, tidak memberikan nilai signifikan untuk perilaku, sehingga tidak dapat digunakan sebagai prediktor. Hasil penelitian ini juga menunjukkan bahwa pengguna cukup sadar akan ancaman keamanan, seperti yang ditunjukkan oleh jawaban rata-rata responden yang menganggap *malware*, *data leakage*, dan *data theft* sebagai ancaman yang cukup serius. Hasil penelitian ini menyederhanakan model perilaku pengguna smartphone dengan menegaskan pentingnya variabel kontekstual, seperti efektivitas tindakan dan ancaman malware, dibandingkan variabel berbasis ekspektasi yang tidak

*Idealis: Indonesia Journal Information System*
**Volume 8, Nomor 1, Januari 2025**
**ISSN 2684-7280 (*online*)**
Halaman 150-159
*available online at* http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/index

signifikan. Temuan ini memiliki implikasi praktis bagi pengembang dan regulator untuk fokus pada ancaman nyata dalam kampanye edukasi dan kebijakan keamanan. Penelitian lanjutan dapat mengeksplorasi relevansi variabel lain dalam konteks atau populasi yang berbeda.

## UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Universitas Multimedia Nusantara khususnya Program Studi Sistem Informasi yang telah memberikan dukungan baik materiil maupun nonmateriil dalam penyusunan artikel ini.

## DAFTAR PUSTAKA

[1] G. Gufran, I. M.-J. (Jurnal I. S. dan, and undefined 2020, "Pemanfaatan e-modul berbasis smartphone sebagai media literasi masyakarat," *ejournal.mandalanursa.orgG Gufran, I MatayaJISIP (Jurnal Ilmu Sosial dan Pendidikan), 2020•ejournal.mandalanursa.org*, 2020, Accessed: Jul. 12, 2024. [Online]. Available: https://ejournal.mandalanursa.org/index.php/JISIP/article/view/1060

[2] D. Pranitasari, A. S.-J. A. D. Manajemen, and undefined 2021, "Analisis Kepuasan Pelanggan Elektronik Shopee menggunakan Metode E-Service Quality dan Kartesius," *ejournal.stei.ac.id*, 2021, Accessed: Jul. 12, 2024. [Online]. Available: https://ejournal.stei.ac.id/index.php/JAM/article/view/438

[3] J. Hasan, "Mempertimbangkan Pendekatan Prinsiplisme dalam Entrepreneurship1," *books.google.comJ HasanRefleksi 30 Tahun HIDESI, 2021•books.google.com2*, 2021, Accessed: Jul. 12, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=n-BCEAAAQBAJ&oi=fnd&pg=PA205&dq=%5B8%5D%09Hasan,+J.+(2021).+Mempertimbangkan+Pendekatan+Prinsiplisme+dalam+Entrepreneurship1.+Refleksi+30+Tahun+HIDESI,+205.&ots=BWzJcvT-A-&sig=O07DMnj4Tcem6x3V0JZZ5Qez9nM

[4] N. Zaidan *et al.*, *Kewirausahaan Era Digital*. 2023. Accessed: Jul. 12, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=iWHZEAAAQBAJ&oi=fnd&pg=PA1&dq=%5B9%5D%09Zaidan,+N.,+Salsabila,+A.,+Fahri,+B.+A.,+Sinaga,+J.+F.,+Syahputra,+R.+A.,+Wadeng,+T.,+...+%26+Al+Azhari,+M.+R.+(2023).+Kewirausahaan+Era+Digital.+Indonesia+Emas+Group.&ots=zSE1iMmsqR&sig=nQPYAqR_AEPU00KrcldeB1VVu3s

[5] Y. Sudaryo, N. Efi, and M. Yosep, *Digital Marketing dan Fintech di Indonesia*. 2020. Accessed: Jul. 12, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=kpD5DwAAQBAJ&oi=fnd&pg=PA1&dq=%5B10%5D%09Yoyo+Sudaryo,+S.+E.,+MM,+M.,+Efi,+N.+A.+S.,+Yosep,+M.+A.,+SE,+M.,+Nurdiansyah,+B.,+%26+ST,+I.+(2020).+Digital+Marketing+dan+Fintech+di+Indonesia.+Penerbit+Andi.&ots=ETwWTNcTWc&sig=xx1rYO0mxgQsZYRbfBVW6HAPPU0

[6] M. Alawida and A. Omolara, "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," *ElsevierM Alawida, AE Omolara, OI Abiodun, M Al-RajabJournal of King Saud University-Computer and Information Sciences, 2022•Elsevier*, 2022, Accessed: Jul. 12, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157822002762

[7] H. Ardianto, "Motif Perempuan Bermain Game Online Pubg Mobile (Studi Pada Kalangan Mahasiswi Fakultas Ilmu Komunikasi Universitas Islam Riau)," 2022, Accessed: Jul. 12, 2024. [Online]. Available: http://repository.uir.ac.id/id/eprint/15224

[8] L. Knapova, A. Kruzikova, L. Dedkova, and D. Smahel, "Who Is Smart with Their Smartphones? Determinants of Smartphone Security Behavior," *Cyberpsychol Behav Soc Netw*, vol. 24, no. 9, pp. 584–592, Sep. 2021, doi: 10.1089/CYBER.2020.0599.

[9] P. Shah and A. Agarwal, "Cybersecurity behaviour of smartphone users in India: an empirical analysis," *Information and Computer Security*, vol. 28, no. 2, pp. 293–318, Jun. 2020, doi: 10.1108/ICS-04-2019-0041/FULL/HTML.

[10] A. Aleroud, E. Abu-Shanab, … A. A.-A.-J. of I., and undefined 2020, "An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities," *ElsevierA Aleroud, E Abu-Shanab, A Al-Aiad, Y AlshboulJournal of Information Security and Applications, 2020•Elsevier*, 2020, Accessed: Nov. 15, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212620307791

[11] F. L. Sylvester, "Mobile device users' susceptibility to phishing attacks," *International Journal of Computer Science and Information Technology (IJCSIT)*, vol. 14, no. 1, 2022, Accessed: Nov. 26, 2024. [Online]. Available: https://www.researchgate.net/publication/358996746_Mobile_device_users'_susceptibility_to_phishing_attacks

[12] N. F. Amin, S. Garancang, ; Kamaluddin Abunawas, N. Penulis, : Nur, and F. Amin, "Konsep umum populasi dan sampel dalam penelitian," *journal.unismuh.ac.idNF Amin, S Garancang, K AbunawasPilar, 2023•journal.unismuh.ac.id*, vol. 14, no. 1, 2023, Accessed: Jul. 12, 2024. [Online]. Available: https://journal.unismuh.ac.id/index.php/pilar/article/view/10624

[13] M. del C. V. Martínez, J.-M. Montero, P. A. M. Cervantes, and P. A. M. Cervantes, "Recent Advances and Applications in Partial Least Squares Structural Equation Modeling (PLS-SEM)," *Recent Advances and Applications in Partial Least Squares Structural Equation Modeling (PLS-SEM)*, p. 494, Dec. 2023, doi: 10.3390/BOOKS978-3-0365-9593-1.

[14] M. Irwansyah, B. W.-J. C. Mandalika, and undefined 2023, "ANALISIS HUBUNGAN ANTARA PROGRAM BEHAVIOR BASED SAFETY (BBS) DAN TINGKAT KEPATUHAN TERHADAP PERILAKU KESELAMATAN KERJA," *ojs.cahayamandalika.comM Irwansyah, B WidanarkoJurnal Cahaya Mandalika ISSN 2721-4796 (online), 2023•ojs.cahayamandalika.com*, 2023, Accessed: Nov. 26, 2024. [Online]. Available: https://ojs.cahayamandalika.com/index.php/jcm/article/view/2553

[15] B. Yusuf, "PENGARUH LAYANAN FINANCIAL TECHNOLOGY BERBASIS METODE PEMBAYARAN PAYLATER TERHADAP PERILAKU IMPLUSIVE BUYING," 2022, Accessed: Nov. 15, 2024. [Online]. Available: http://digilib.unila.ac.id/id/eprint/67838