# Analisa Perilaku Keamanan Informasi Pengguna Mobile Banking

**Sintaria Sembiring[1], Henry Pandia[2*]**
[1,2] Fakultas Teknologi Informasi, Universitas Advent Indonesia
e-mail: [1]sintaria.sembiring@unai.edu, [2*]pandiahenry@unai.edu

**Abstrak**

Penggunaan layanan mobile banking bertumbuh dengan pesat dan telah merevolusi sektor perbankan, menawarkan pelanggan akses yang nyaman dan efisien ke layanan perbankan tanpa batasan waktu dan jarak. Namun, kenyamanan ini disertai dengan risiko keamanan informasi. Karena itu perilaku keamanan informasi pengguna penting untuk meminimalkan resiko dan dampaknya. Penelitian ini bertujuan menganalisa perilaku keamanan informasi pengguna mobile banking di Indonesia, dengan fokus pada faktor-faktor yang mempengaruhi perilaku tersebut.

Penelitian ini melakukan survey terhadap 365 responden pengguna aplikasi mobile banking dengan gender, umur, tingkat pendidikan, dan preferensi aplikasi mobile banking yang beragam. Penelitian ini mengukur lima dimensi perilaku keamanan informasi, yaitu: manajemen password, penggunaan aplikasi pesan, penggunaan internet, penggunaan perangkat di ruang publik, dan pelaporan insiden.

Penelitian menemukan bahwa perilaku keamanan informasi pengguna mobile banking mempunyai keberagaman yang signifikan. Temuan ini menekankan pentingnya bank mengintegrasikan perilaku pengguna ke dalam strategi keamanan informasi yang komprehensif. Penelitian ini berkontribusi dalam meningkatkan praktik keamanan informasi di mobile banking dengan memberikan wawasan tentang perilaku pengguna dan pengaruh demografis.

**Kata Kunci:** perilaku keamanan informasi, mobile banking, resiko, kewaspadaan keamanan informasi

# *Analysis of Information Security Behaviors of Mobile Banking Users*

***Abstract***

*The use of mobile banking services has grown rapidly and revolutionized the banking sector, offering customers convenient and efficient access to banking services without time and distance limitations. However, this convenience comes with information security risks. Therefore, user information security behavior is crucial to minimize these risks and their impacts. This study aims to analyze the information security behaviors of mobile banking users in Indonesia, focusing on the factors that influence these behaviors.*

*This research surveyed 365 respondents who use mobile banking applications, with diverse genders, ages, education levels, and mobile banking application preferences. The study measured five dimensions of information security behavior: password management, messaging app usage, internet usage, devices usage in public, and incident reporting.*

*The research found that information security behaviors among mobile banking users vary significantly. These findings highlight the importance of banks integrating user behaviors into comprehensive information security strategies. This study contributes to enhancing information security practices in mobile banking by providing insights into user behaviors and demographic influences.*

***Keywords:*** *information security behavior, mobile banking, risks, information security awareness*

## 1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam sektor perbankan. Teknologi informasi dan komunikasi digunakan untuk mendukung operasional dan memberikan layanan perbankan. Salah satu bentuk layanan perbankan yang berkembang dan digunakan secara luas adalah layanan mobile banking. Penggunaan layanan ini meningkat secara dramatis dalam beberapa tahun terakhir seiring dengan semakin luasnya jangkauan internet dan bertambahnya pengguna telepon pintar. Aplikasi mobile banking memberikan akses kepada nasabah layanan perbankan yang mudah, efisien dan tidak dibatasi jarak dan waktu. Melalui aplikasi mobile banking, penggunaan dapat melakukan berbagai transaksi dan menggunakan berbagai fitur layanan lainnya [1].

Dibalik kemudahan yang ditawarkan oleh layanan mobile banking, terdapat tantangan dan resiko yang harus diwaspadai, baik oleh bank sebagai pemberi layanan maupun nasabah sebagai pengguna layanan. Resiko keamanan informasi merupakan masalah utama bagi bank dan pengguna layanan karena inovasi teknologi tersebut menyisakan celah keamanan [2]. Bahaya pencurian data, serangan malware, penipuan berbasis teknologi, dan akses yang oleh yang tidak berhak menjadi ancaman yang harus diwaspadai oleh pengguna aplikasi mobil banking [3].

Sistem perbankan telah menyediakan berbagai solusi keamanan informasi untuk penggunaan mobile dan online banking. Berbagai teknologi keamanan informasi terus dikembangkan untuk mendapatkan sistem keamanan yang lebih baik. Namun meskipun demikian, teknologi keamanan informasi harus didukung oleh kewaspadaan keamanan informasi dari penggunanya. Penelitian sebelumnya [4, 5, 6, 7, 8] menyimpulkan bahwa faktor manusia merupakan faktor yang paling dominan penyebab terjadinya pelanggaran keamanan informasi. Faktor manusia seperti social engineering, budaya keamanan informasi yang buruk, pengelolaan password yang beresiko, stress, kelelahan kerja dan kelelahan keamanan seringkali menjadi penyebab terjadinya pelanggaran keamanan informasi [2].

Mengingat resiko dan dampak serangan keamanan informasi dalam bidang perbankan, dan bagaimana faktor manusia merupakan faktor yang penting diperhatikan, Peneliti sebelumnya [9] menyarankan agar bank penyedia layanan memperhatikan faktor-faktor kritis manusia untuk meminimalkan suksesnya serangan keamanan, mengurangi resiko dan biaya pemulihan dari serangan tersebut. Bank harus menjadikan perilaku keamanan informasi dari pengguna aplikasi mobile banking sebagai bagian dari strategi keamanan informasinya.

Perilaku keamanan informasi mencakup tindakan yang dilakukan oleh pengguna mobile banking untuk melindung data peribadi dan finansial mereka dari ancaman akses dari orang yang tidak berhak. Tindakan tersebut mencakup pengelolaan kata sandi, kesadaran adanya usaha *phising*, membagikan data, kewaspadaan mengakses internet di tempat umum, dan pelaporan insiden keamanan informasi. Perilaku keamanan informasi yang baik akan dapat membantu penyedia layanan mobile banking merancang sistem keamanan yang lebih baik serta memberikan edukasi kepada pengguna untuk meningkatkan kesadaran keamanan informasi pengguna untuk mencegah serangan keamanan informasi [10].

Penelitian ini bertujuan untuk menganalisis perilaku keamanan informasi pengguna mobile banking, dengan fokus pada faktor-faktor yang mempengaruhi perilaku tersebut. Penelitian ini juga akan mengeksplorasi pengaruh demografi pengguna seperti jenis kelamin, umur, dan tingkat pendidikan terhadap perilaku keamanan informasi mereka. Penelitian ini akan mempelajari dimensi-dimensi yang merupakan refleksi dari perilaku keamanan informasi, seperti manajemen password (MP), penggunaan aplikasi pengiriman pesan (APP), penggunaan internet (PI), penggunaan perangkat di ruang publik (ADP) dan pelaporan keamanan informasi.

Analisa perilaku keamanan informasi pengguna mobile banking diharapkan dapat memberikan konstribusi yang signifikan dalam upaya meningkatkan keamanan informasi dan kenyamanan pengguna layanan mobile banking. Temuan dari penelitian ini dapat digunakan oleh penyedia layanan mobil banking

sebagai acuan untuk mengembangkan strategi, kebijakan dan panduan praktek keamanan informasi. Penelitian ini juga diharapkan dapat memberikan wawasan yang baru bagi peneliti dan praktisi dalam bidang keamanan informasi untuk dapat memahami perilaku pengguna dalam konteks keamanan informasi.

## 2. Metode Penelitian

### 2.1 Sample

Penelitian ini dilakukan dengan membagikan survey perilaku keamanan informasi dari pengguna aplikasi mobile banking di Indonesia. Survey dilakukan secara digital menggunakan Google Form. Sampel penelitian diperoleh dengan cara mengirimkan link survey melalui aplikasi pengiriman pesan WhatsApp oleh 37 peserta kelas Manajemen Resiko dan Sekuriti Teknologi Informasi kepada orang yang ada di daftar kontak atau grup yang mereka ikuti.

Pemilihan WhatsApp sebagai media distribusi survei dilakukan dengan pertimbangan bahwa platform ini adalah salah satu aplikasi pesan instan yang paling banyak digunakan di Indonesia. WhatsApp memungkinkan penyebaran survei secara cepat dan luas, menjangkau berbagai kalangan masyarakat. Namun, metode ini juga dapat menimbulkan bias karena survei hanya menjangkau pengguna yang aktif di WhatsApp, yang mungkin tidak sepenuhnya mewakili populasi pengguna mobile banking secara umum. Untuk meminimalkan bias ini, upaya dilakukan untuk menyebarkan survei ke berbagai grup dan komunitas di WhatsApp yang memiliki keragaman demografis yang cukup.

Ada 387 responden yang berpartisipasi dalam penelitian ini dan 365 kuisoner dinyatakan valid. Ukuran sampel sebanyak 365 responden dinilai telah mencapai tingkat kepercayaan dan margin of error yang memadai. Data demografi responden dapat dilihat di Tabel 1. Berdasarkan jenis kelamin, 208 responden adalah laki-laki dan 157 orang adalah perempuan. Berdasarkan usia terdapat 9 responden termasuk dalam kelompok usia 60-65 tahun (Baby Boomers), 29 responden berada pada rentang usia 44-59 tahun (Generasi X), 68 responden berada pada rentang usia 28-43 tahun (Generasi Y), dan sebagian besar responden, yaitu 259 orang, masuk dalam kelompok usia 18-27 tahun (Generasi Z). Sampel dinilai telah mewakili beragam demografi dan cukup merepresentasikan pola perilaku pengguna mobile banking di Indonesia.

**Tabel 1** Demografi Responden

| Karateristik | Kategori | Jumlah | Persentase (%) |
|---|---|---|---|
| Jenis Kelamin | Laki-laki | 208 | 56,99 |
| | Perempuan | 157 | 43,01 |
| Umur | 60-65 (Baby Boomers) | 9 | 2,47 |
| | 44-59 (Gen X) | 29 | 7,95 |
| | 28-43 (Gen Y) | 68 | 18,63 |
| | 18-27 (Gen Z) | 259 | 70,96 |
| Tingkat Pendidikan | SMA | 151 | 41,37 |
| | Diploma/Sarjana | 192 | 52,60 |
| | Magister | 17 | 4,66 |
| | Doktor | 5 | 1,37 |
| Aplikasi Mobile Banking | BCA Mobile Banking | 119 | 32,60 |
| | BNI Mobile Banking | 43 | 11,78 |
| | BRI Mobile | 103 | 28,22 |
| | Livin' Mandiri | 78 | 21,37 |
| | Lain-lain | 22 | 6,03 |
| Jumlah Responden | | 365 | 100 |

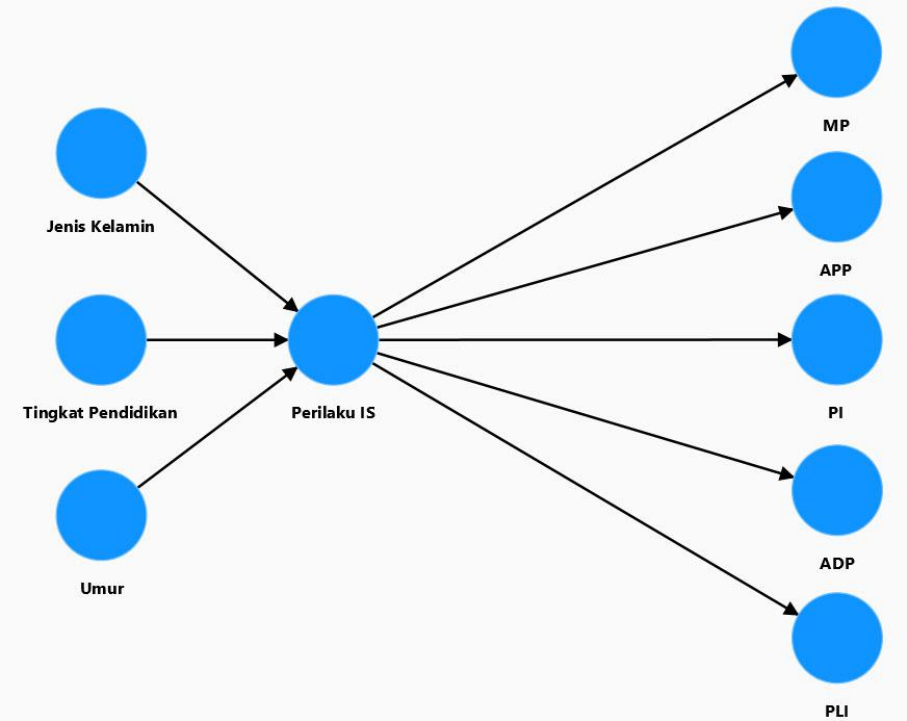
Jika dikelompokkan berdasarkan tingkat pendidikan, mayoritas responden memiliki latar belakang pendidikan Diploma/Sarjana sebanyak 192 orang, diikuti oleh responden dengan tingkat pendidikan SMA sebanyak 151 orang. Sementara itu, terdapat 17 responden yang memiliki gelar Magister dan 5 responden dengan gelar Doktor.

Dalam hal preferensi aplikasi mobile banking, sebagian besar responden menggunakan BCA Mobile Banking sebanyak 119 orang, diikuti oleh BRI Mobile sebanyak 103 orang, Livin' Mandiri sebanyak 78 orang, BNI Mobile Banking sebanyak 43 orang, dan aplikasi lainnya sebanyak 22 orang.

Secara keseluruhan, data demografi responden menunjukkan keragaman dalam aspek jenis kelamin, rentang usia, tingkat pendidikan, dan preferensi aplikasi mobile banking yang digunakan. Demografi responden yang beragam ini memberikan gambaran yang komprehensif tentang karakteristik pengguna aplikasi mobile banking di era digital saat ini.

## 2.2 Model Riset

Penelitian ini mengukur perilaku keamanan informasi (Perilaku IS) menggunakan lima dimensi antara lain: manajemen password (MP), pengelolaan aplikasi pengiriman pesan (APP), penggunaan internet (PI), penggunaan perangkat di ruang publik (ADP) dan pelaporan insiden keamanan informasi (PLI). Selain itu, penelitian ini juga mengukur pengaruh jenis kelamin, umur dan tingkat pendidikan terdapat perilaku keamanan informasi. Model riset untuk penelitian ini ditunjukkan oleh Gambar 1.




**Gambar 1** Model riset

## 2.3 Instrumen Penelitian

Penelitian ini dilakukan untuk mengukur perilaku keamanan informasi pengguna mobile banking. Perangkat survey dikembangkan dengan mengacu kepada perangkat survey Human Aspect of Information Security Questionanaire (HAIS-Q) [11]. HAIS-Q mengukur kesadaran keamanan informasi pengguna teknologi informasi pada 7 bidang area: manajemen password, penggunaan email, penggunaan internet,

penggunaan media sosial, penggunaan perangkat mobile, penanganan informasi dan pelaporan insiden. Karena dinilai kurang relevan dengan kasus di penelitian ini, aspek penggunaan media sosial dan penanganan informasi tidak gunakan pada penelitian ini dan hanya menggunakan 5 fokus area yang lain.

Menggunakan lima fokus area, penelitian ini memodifikasi pertanyaan yang ada. Selain itu, terminologi yang digunakan disesuaikan dengan penggunaan aplikasi mobile banking. Dimensi dan pertanyaan yang digunakan pada survey penelitian ini ditunjukkan oleh Tabel 2.

**Tabel 2** Karateristik untuk Konstruk Utama

| No | Kode | Dimensi/Item pertanyaan |
|---|---|---|
| 1 | **MP** | **Manajemen Password** |
| 2 | B1 | Penggunaan password yang berbeda untuk akun media sosial dan akun mobile banking. |
| 3 | B2 | Membagikan password akun mobile banking dengan keluarga atau teman. |
| 4 | B3 | Menggunakan password yang kuat. |
| 5 | **APP** | **Penggunaan aplikasi pengiriman pesan** |
| 6 | B4 | Tidak mengeklik link yang dikirimkan bersama email atau pesan secara sembarangan |
| 7 | B5 | Tidak membuka email atau pesan dari orang yang tidak dikenal secara sembarangan |
| 8 | B6 | Tidak membuka file yang ada disertakan di email atau pesan yang berasal dari orang yang tidak dikenal. |
| 9 | **PI** | **Penggunaan Internet** |
| 10 | B7 | Men-download aplikasi mobile banking dari sumber yang terpercaya |
| 11 | B8 | Tidak mengeklik link yang dikirimkan melalui email atau pesan dari sumber yang tidak jelas. |
| 12 | B9 | Mengecek keabsahan sebuah website sebelum memasukkan informasi |
| 13 | **ADP** | **Akses di ruang publik** |
| 14 | B10 | Tidak meletakkan dan meninggalkan perangkat di tempat umum tanpa pengawasan |
| 15 | B11 | Tidak mengakses akun mobile banking menggunakan WiFi publik |
| 16 | B12 | Memastikan tidak ada yang mengintip/melihat ketika membuka akun mobile banking di tempat umum |
| 17 | **PLI** | **Pelaporan insiden keamanan SI** |
| 18 | B13 | Melaporkan ke pihak bank jika menemukan seseorang yang tidak berhak sedang berusaha mendapatkan hak akses ke akun mobile banking. |
| 19 | B14 | Melaporkan kepada pihak bank jika terjadi insiden keamanan, akses yang tidak berhak atau pelanggaran aturan pada akun mobile banking saya. |
| 20 | B15 | Melaporkan ke bank ketika menemukan adanya transaksi yang terjadi di akun mobil banking oleh orang yang tidak berhak |
| 21 | **Perilaku IS** | **Perilaku keamanan sistem informasi** |

## 2.4 Pengujian Model

Pada penelitian ini, pengujian reliabilitas dan validitas dari alat ukur yang digunakan dilakukan dengan menggunakan nilai Cronbach's alpha, composite reliability (rho_a), composite reliability (rho_c) dan average variance extracted (AVE) untuk masing-masing dimensi. Hasil pengujian reliabilitas dan validitas tersebut ditampilkan di Tabel 3.

Mengacu kepada Tabel 3 hasil pengujian realibilitas dan validitas konstruk, diperoleh nilai Cronbach's alpha untuk dimensi pengelolaan aplikasi pengiriman pesan (APP) dan manajemen password adalah 0.695 dan 0.700 dinyatakan dapat diterima. Sedangkan nilai Cronbach's alpha untuk dimensi yang lain lebih besar dari 0. 700 dan dinyatakan baik [12]. Karena itu, nilai Cronbach's alpha mengindikasikan bahwa dimensi dan konstruk yang ada mempunyai reliabilitas internal yang baik.

**Tabel 3** Reliabilitas dan validitas konstruk

| Dimensi | Cronbach's alpha | Composite reliability (rho_a) | Composite reliability (rho_c) | Average variance extracted (AVE) |
|---|---|---|---|---|
| ADP | 0,836 | 0,837 | 0,904 | 0,759 |
| APP | 0,695 | 0,776 | 0,826 | 0,620 |
| MP | 0,700 | 0,703 | 0,833 | 0,624 |
| PI | 0,739 | 0,766 | 0,851 | 0,656 |
| PLI | 0,945 | 0,948 | 0,965 | 0,902 |
| Perilaku IS | 0,799 | 0,809 | 0,842 | 0, 627 |

Nilai reliabilitas komposit yang ideal adalah 0.7. Mengacu kepada nilai reliabilitas komposit (rho_a dan rho_c) dari hasil pengujian menunjukkan bahwa semua dimensi dan konstruk memiliki nilai (rho_a dan rho_c yang lebih besar dari 0.7. Karena itu, semua dimensi dan konstruk memiliki reliabilitas komposit yang memadai.

Nilai Average Variance Extracted (AVE) digunakan untuk mengukur validitas konvergen dari sebuah dimensi dan kontruk. Hasil pengujian menunjukkan nilai AVE untuk semua dimensi lebih besar dari 0.5 memiliki validitas konvergen yang baik. Dimensi pelaporan insiden keamanan informasi (PLI) yang sangat tinggi (0,902), menunjukkan validitas konvergen yang sangat kuat.

Secara keseluruhan tingkat reliabilitas dan validitas dari dimensi dan konstruk yang diukur dinilai memadai dan dapat diterima. Karena itu disimpulkan bahwa alat ukur yang digunakan reliabel dan valid.

**Tabel 4** Kriteria Fornell-Larcker

| Item Pengukuran | ADP | APP | Gender | MP | PI | PLI | Perilaku IS | Pendidikan | Umur |
|---|---|---|---|---|---|---|---|---|---|
| ADP | **0,871** | | | | | | | | |
| APP | 0,463 | **0,788** | | | | | | | |
| Gender | 0,024 | 0,072 | **1,000** | | | | | | |
| MP | 0,347 | 0,362 | 0,082 | **0,790** | | | | | |
| PI | 0,040 | 0,081 | 0,070 | 0,322 | **0,810** | | | | |
| PLI | 0,046 | 0,003 | -0,045 | 0,157 | 0,447 | **0,950** | | | |
| Perilaku IS | 0,642 | 0,609 | 0,063 | 0,724 | 0,582 | 0,526 | **0,517** | | |
| Tingkat Pendidikan | 0,012 | -0,052 | -0,104 | 0,026 | -0,023 | 0,043 | 0,006 | **1,000** | |
| Umur | -0,088 | 0,059 | 0,095 | -0,095 | 0,077 | 0,014 | -0,022 | -0,411 | **1,000** |

Analisis Fornell-Larcker menunjukkan matriks korelasi antara variabel-variabel yang ada, menggambarkan tingkat signifikan hubungan antara setiap pasangan variabel. Tabel 4 di atas menunjukkan nilai validitas diskriminan dari konstruk yang diukur dalam penelitian ini. Nilai diagonal yang dicetak tebal merupakan akar kuadrat dari Average Variance Extracted (AVE) untuk setiap konstruk, sedangkan nilai di luar diagonal adalah korelasi antar dimensi atau konstruk. Mengacu kepada nilai di atas, semua nilai diagonal lebih besar dari nilai korelasi di baris dan kolom yang sama, menunjukkan bahwa setiap konstruk memiliki validitas diskriminan yang memadai [13].

Mengacu kepada nilai hubungan antar konstruk, dapat disimpulkan bahwa konstruk perilaku keamanan informasi (Perilaku IS) mempunyai hubungan yang kuat dengan dimensi manajemen password (MP), penggunaan aplikasi pengiriman pesan, penggunaan internet, penggunaan perangkat di ruang publik (ADP) dan pelaporan insiden keamanan informasi (PLI) dengan nilai kriteria Fornell-Larcker berada dalam rentang 0,526 sampai 0,724.

Hasil pengujian menunjukan variabel demografi seperti gender, umur dan tingkat pendidikan memiliki korelasi yang sangat rendah dengan konstruk perilaku keamanan informasi (Perilaku IS). Ini menunjukkan bahwa faktor demografi tidak mempunyai pengaruh signifikan terhapat perilaku keamanan informasi.

Pengujian *cross loading* digunakan untuk mengukur seberapa baik item-item pengukuran untuk setiap dimensi mempunyai hubungan yang kuat dengan dimensi yang diukurnya. Nilai *cross loading* ditunjukkan oleh Tabel 5. Di Tabel 5 dapat dilihat bahwa pertanyaan B1 sampai B3 mempunyai hubungan yang kuat dengan dimensi manajemen password (MP), pertanyaan B4 sampai B6 mempunyai hubungan yang kuat dengan dimensi penggunaan aplikasi pengiriman pesan (AAP), demikian juga dengan pertanyaan B7 sampai B15, mempunyai hubungan yang kuat dengan masing-masing dimensi yang diukur. Karena itu disimpulkan bahwa masing-masing dimensi memiliki validitas diskriminan yang baik.

**Tabel 5** Cross Loading

| Item Pengukuran | MP | APP | PI | ADP | PLI | Gender | Umur | Pendidikan | Perilaku IS |
|---|---|---|---|---|---|---|---|---|---|
| B1 | **0,816** | 0,290 | 0,310 | 0,287 | 0,152 | 0,063 | -0,070 | 0,022 | 0,612 |
| B2 | **0,782** | 0,355 | 0,230 | 0,289 | 0,091 | 0,095 | -0,057 | 0,024 | 0,577 |
| B3 | **0,772** | 0,207 | 0,217 | 0,242 | 0,130 | 0,033 | -0,102 | 0,015 | 0,522 |
| B4 | 0,168 | **0,579** | -0,112 | 0,280 | -0,083 | -0,050 | -0,039 | 0,014 | 0,270 |
| B5 | 0,295 | **0,880** | 0,076 | 0,389 | 0,023 | 0,070 | 0,054 | -0,044 | 0,529 |
| B6 | 0,355 | **0,867** | 0,140 | 0,413 | 0,024 | 0,099 | 0,083 | -0,067 | 0,573 |
| B7 | 0,203 | 0,045 | **0,807** | 0,050 | 0,341 | 0,088 | 0,073 | -0,044 | 0,444 |
| B8 | 0,256 | 0,040 | **0,748** | -0,038 | 0,278 | -0,023 | 0,031 | 0,012 | 0,392 |
| B9 | 0,314 | 0,101 | **0,870** | 0,068 | 0,445 | 0,088 | 0,078 | -0,021 | 0,558 |
| B10 | 0,282 | 0,428 | 0,120 | **0,751** | 0,074 | 0,059 | -0,051 | -0,032 | 0,552 |
| B11 | 0,297 | 0,390 | -0,035 | **0,923** | 0,027 | -0,017 | -0,096 | 0,026 | 0,548 |
| B12 | 0,322 | 0,389 | 0,019 | **0,929** | 0,020 | 0,019 | -0,083 | 0,036 | 0,572 |
| B13 | 0,125 | 0,000 | 0,400 | 0,030 | **0,935** | -0,039 | 0,048 | 0,030 | 0,473 |
| B14 | 0,154 | -0,018 | 0,417 | 0,041 | **0,962** | -0,055 | -0,005 | 0,054 | 0,496 |
| B15 | 0,167 | 0,026 | 0,454 | 0,059 | **0,951** | -0,034 | -0,002 | 0,038 | 0,527 |
| Gender | 0,082 | 0,072 | 0,070 | 0,024 | -0,045 | **1,000** | 0,095 | -0,104 | 0,063 |
| Umur | -0,095 | 0,059 | 0,077 | -0,088 | 0,014 | 0,095 | **1,000** | -0,411 | -0,022 |
| Pendidikan | 0,026 | -0,052 | -0,023 | 0,012 | 0,043 | -0,104 | -0,411 | **1,000** | 0,006 |

Analisa validitas diskriminan juga menunjukkan bahwa dimensi manajemen password (MP), penggunaan perangkat di ruang publik (ADP), dan pelaporan insiden keamanan informasi (PLI) mempunyai konstribusi yang signifikan terhadap konstruk utama perilaku keamanan informasi (Perilaku IS) yang ditunjukkan dengan nilai *cross loading* yang tinggi. Dimensi penggunaan aplikasi pengiriman pesan (APP) dan penggunaan internet (PI) mempunyai hubungan moderat dengan perilaku keamanan informasi (Perilaku IS). Sedangkan variabel gender, umur dan tingkat pendidikan tidak mempunyai pengaruh yang signifikan terhadap konstruk perilaku keamanan informasi (perilaku IS).

Berdasarkan pengujian nilai Fornell Lacker dan *cross loading* di atas, penelitian ini menyimpulkan alat ukur yang digunakan memiliki validitas dan reliabilitas yang baik untuk mengukur dimensi dan konstruk yang ada.

## 3. Hasil Penelitian

### 3.1 Statistik Deskriptif

Penelitian ini menggunakan statistik deskriptif untuk merangkum dan menggambarkan karakteristik data dari hasil survei yang digunakan. Nilai rerata digunakan untuk mengetahui rata-rata tanggapan

responden terhadap item pertanyaan. Sedangkan nilai standar deviasi digunakan untuk mengukur variasi tanggapan responden. Nilai rerata dan standar deviasi hasil survey ditunjukkan oleh Tabel 6.

**Tabel 6** Nilai rerata dan standar deviasi

| No | Kode | Rerata | Std Deviasi |
|---|---|---|---|
| I | MP | 3.497 | |
| 1 | B1 | 3.420 | 1.163 |
| 2 | B2 | 3.692 | 1.114 |
| 3 | B3 | 3.379 | 1.071 |
| II | APP | 4.048 | |
| 4 | B4 | 3.628 | 1.148 |
| 5 | B5 | 4.158 | 1.034 |
| 6 | B6 | 4.359 | 0,950 |
| II | PI | 3.745 | |
| 7 | B7 | 3.967 | 1.427 |
| 8 | B8 | 3.384 | 1.583 |
| 9 | B9 | 3.885 | 1.278 |
| IV | ADP | 3.935 | |
| 10 | B10 | 4.155 | 1.091 |
| 11 | B11 | 3.875 | 1.062 |
| 12 | B12 | 3.774 | 1.111 |
| V | PLI | 3.280 | |
| 13 | B13 | 3.198 | 1.514 |
| 14 | B14 | 3.293 | 1.498 |
| 15 | B15 | 3.349 | 1.564 |

Tabel 6 di atas menunjukkan bahwa dari kelima dimensi yang diukur, dimensi penggunaan aplikasi pengiriman pesan (APP) memiliki rerata paling tinggi dengan standar deviasi yang kecil. Ini menunjukkan bahwa pengguna mobile banking memiliki perilaku keamanan informasi yang baik dalam hal penggunaan aplikasi pengiriman pesan. Nilai standar deviasi yang kecil menunjukkan perilaku tersebut relatif seragam. Perilaku keamanan informasi yang sama namun dengan rerata yang sedikit lebih rendah ditemukan pada dimensi penggunaan perangkat di ruang publik (ADP).

Nilai rerata untuk dimensi penggunaan internet (PI) menunjukkan nilai yang cukup tinggi namun mempunyai standar deviasi yang tinggi. Ini mencerminkan perilaku penggunaan internet oleh pengguna mobile banking memiliki keberagaman yang signifikan. Sedangkan nilai rerata untuk dimensi manajemen password (MP) berada pada level cukup dengan tingkat keberagamana yang rendah.

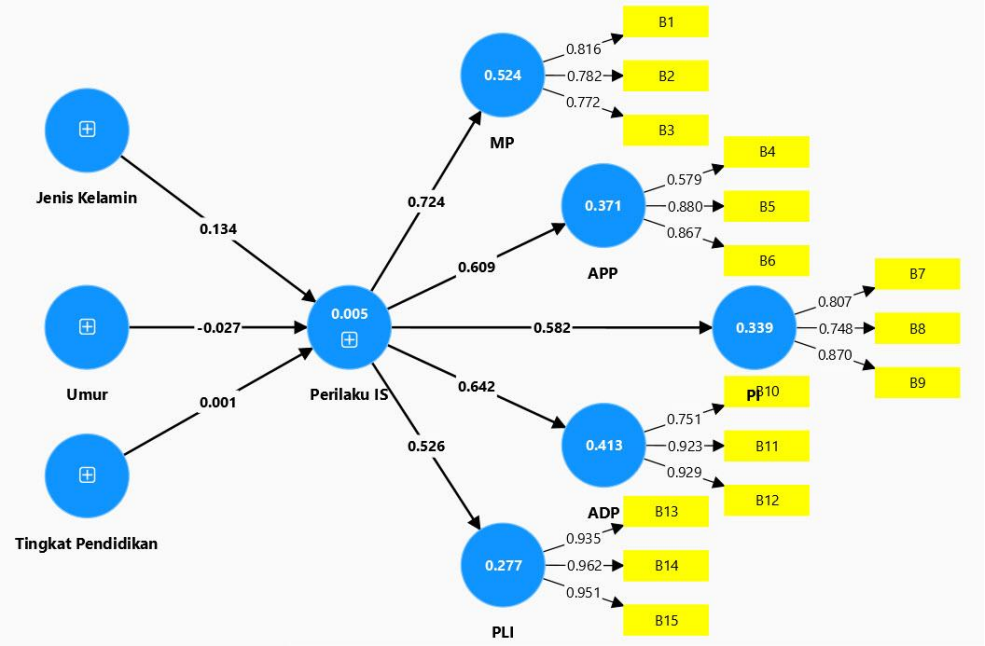
Nilai rerata pada dimensi pelaporan insiden keamanan informasi merupakan nilai yang paling rendah dibanding dengan semua dimensi yang lain. Selain itu, dimensi ini memiliki standar deviasi yang tinggi. Ini menunjukkan sebagian pengguna tidak mau melaporkan insiden keamanan informasi yang mereka temukan.

### 3.2 Koefisien Jalur

Analisa koefisien jalur *(path coefficient)* digunakan untuk memahami hubungan antara variabel-variabel yang diukur dengan konstruk perilaku keamanan informasi (Perilaku IS). Koefisien jalur dihitung dengan menggunakan Smart PLS dan hasil perhitungan ditunjukkan oleh Gambar 2 di bawah ini.

Nilai koefisien jalur jenis kelamin dengan perilaku keamanan informasi (Perilaku IS) adalah 0,134 yang menunjukkan adanya hubungan positif diantara kedua konstruk. Namun hubungan tersebut dinilai kecil dan tidak signifikan. Sedangkan koefisien jalur untuk dimensi umur dan tingkat pendidikan dengan Perilaku IS adalah -0,027 dan 0,001, sehingga disimpulkan tidak ada hubungan antara kedua dimensi tersebut dengan konstruk utama.

Koefisien jalur untuk dimensi manajemen password (MP), penggunaan aplikasi pengiriman pesan (APP), penggunaan internet (PI), penggunaan perangkat di ruang publik (ADP) dan pelaporan insiden keamanan informasi (PLI) dengan konstruk utama perilaku keamanan infomrasi (perilaku IS) berada pada rentang 0,526 dan 0,724. Ini menunjukkan adanya hubungan yang kuat antara masing-masing dimensi dengan konstruk utama. Jika ingin meningkatkan perilaku keamanan informasi pengguna mobile banking, maka pihak bank dapat memberikan edukasi kepada pengguna dalam bidang manajemen password, penggunaan aplikasi pengiriman pesan, penggunaan internet, penggunaan perangkat di ruang publik dan pelaporan insiden keamanan informasi.




**Gambar 2** Nilai koefien jalur

## 4. Pembahasan

Nilai rerata tertinggi pada dimensi penggunaan aplikasi pengirman pesan (APP) menunjukkan bahwa pengguna mobile banking cenderung memiliki perilaku keamanan informasi yang baik dalam hal penggunaan aplikasi pengiriman pesan. Mengacu kepada penelitian sebelumnya [14] hal ini bisa terjadi karena adanya edukasi dan kesadaran pengguna tentang keamanan aplikasi pengiriman pesan. Maraknya penipuan dan pelanggaran keamanan informasi melalui aplikasi pengiriman pesan telah memberikan edukasi bagi pengguna yang mendorong meningkatkan perilaku keamanan informasi secara signifikan.

Dimensi penggunaan perangkat di ruang publik menunjukkan rerata yang tinggi dengan standar deviasi yang rendah, mengindikasikan perilaku yang relatif seragam di antara pengguna. Ruang publik di Indonesia yang relatif tidak aman terhadap pencurian perangkat teknologi, menyebabkan tingkat kewaspadaan pengguna menjadi meningkatkan. Hal ini sejalan dengan hasil penelitian terdahulu [15] yang menyimpulkan bahwa penggunaan perangkat di ruang publik adalah area kritis dalam keamanan informasi, sehingga membutuhkan tingkat kesadaran keamanan informasi yang baik sebagai tindakan pencegahan terhadap insiden keamanan informasi.

Dimensi penggunaan internet (PI) menunjukkan rerata yang cukup tinggi dengan standar deviasi yang tinggi, yang mencerminkan keberagaman perilaku di kalangan pengguna. Temuan ini konsisten dengan penelitian sebelumnya [10], yang menemukan bahwa perilaku penggunaan internet bervariasi secara signifikan tergantung pada tingkat kesadaran dan pemahaman pengguna terhadap resiko keamanan informasi.

Penelitian menemukan bahwa dimensi manajemen password memiliki rerata yang cukup dengan tingkat keberagaman yang rendah. Manajemen password yang baik merupakan hal yang sangat penting untuk meningkatkan keamanan informasi [3]. Karena itu, perbankan perlu menerapkan mekanisme manajemen password yang baik seperti menerapkan aturan penggunaan password yang kuat, pergantian password yang berkala dan memberikan edukasi kepada pengguna tentang pentingnya manajemen password. Hal ini penting selaras dengan temuan peneliti sebelumnya [14] bahwa manajemen password yang baik sangat berpengaruh terhadap keamanan informasi secara keseluruhan .

Penelitian menemukan bahwa aspek pelaporan insiden keamanan informasi memiliki rerata terendah dan standar deviasi yang tinggi. Ini menunjukkan bahwa pengguna mobile banking tidak mau atau tidak terbiasa melaporkan insiden keamanan informasi. Hal ini dapat terjadi dikarenakan mekanisme pelaporan yang rumit dan adanya dampak pembekuan akun pengguna sementara yang tidak diinginkan oleh pengguna. Aspek ini tidak dapat ditingkatkan hanya dengan memberikan edukasi kepada pengguna, melainkan harus ditangani dengan membuat mekanisme pelaporan yang lebih sederhana, dan penanganan laporan yang cepat sehingga pembekuan akun pengguna tidak terlalu lama.

Rendahnya perilaku keamanan informasi khususnya pada aspek pelaporan insiden keamanan perlu mendapat perhatian serius dari bank. Pelaporan insiden keamanan penting untuk mencegah dampak resiko yang lebih besar dan juga terjadinya insiden serupa. Selain itu, pelaporan insiden dapat menjadi umpan balik baik bank untuk memperbaiki sistem keamanan informasi yang ada. Hal ini didukung oleh penelitian sebelumnya [1], yang menekankan bahwa pelaporan insiden adalah aspek krusial dalam memperkuat keamanan keseluruhan sistem kemanan informasi perbankan.

Analisa koefisien jalur menunjukkan bahwa hubungan yang kuat antara perilaku keamanan informasi dengan dimensi manajemen password (MP), pengelolaan aplikasi pengiriman pesan (APP), penggunaan internet (PI), penggunaan perangkat di ruang publik (ADP) dan pelaporan insiden keamanan informasi (PLI). Jika bank ingin meningkatkan perilaku keamanan informasi pengguna mobile banking, bank perlu fokus pada edukasi dan peningkatan kesadaran pengguna pada kelima dimensi tersebut. Penelitian terdahulu [6] menyarankan program peningkatan kewaspadaan keamanan informasi, training dan pendidikan dapat digunakan sebagai strategi utama untuk meningkatkan perilaku keamanan informasi pengguna.

Penelitian ini menemukan bahwa faktor demografi gender, umur dan tingkat pendidikat tidak memiliki hubungan yang signifikan dengan perilaku keamanan informasi pengguna mobile banking. Temuan ini selaras dengan hasil penelitian [9] sebelumnya yang menyimpulkan bahwa faktor-faktor demografi seringkali tidak berpengaruh signifikan terhadap perilaku keamanan informasi, tetapi lebih dipengaruhi oleh faktor-faktor psikologis dan edukasi. Secara teoritis, penelitian ini memperkuat konsep bahwa faktor demografis tidak mempengaruhi perilaku keamanan informasi pengguna.

Berdasarkan temuan di atas, penelitian ini memberikan rekomendasi praktis agar bank sebagai pengembang aplikasi mobile banking dapat memberikan program pendidikan atau pelatihan kepada pengguna untuk meningkatkan kesadaran keamanan informasi pengguna. Program dapat mencakup simulasi atau latihan praktis yang menggambarkan situasi nyata untuk membantu pengguna memahami berbagai ancaman keamanan informasi dan cara mengatasinya. Selain itu, bank juga dapat meningkatkan komunikasi dan sosialisasi keamanan informasi melalui berbagai saluran komunikasi seperti aplikasi pengiriman pesan, email dan media sosial. Dengan menerapkan rekomendasi ini diharapkan bank dapat meningkatkan perilaku keamanan informasi pengguna mobile banking.

## 5. Kesimpulan

Penelitian ini menyimpulkan pentingnya beberapa dimensi yang mempengaruhi perilaku keamanan informasi pengguna mobile banking. Edukasi dan peningkatan kesadaran dalam hal manajemen password, penggunaan aplikasi pengiriman pesan, penggunaan internet, penggunaan perangkat di ruang publik, dan pelaporan insiden keamanan sangat diperlukan untuk memperkuat keamanan informasi pengguna.

Upaya lebih lanjut diperlukan untuk mengatasi hambatan dalam pelaporan insiden keamanan, yang terbukti menjadi area paling lemah dalam perilaku keamanan informasi pengguna. Sebagai rekomendasi, bank perlu membangun mekanisme pelaporan insiden keamanan informasi yang lebih praktis dan ramah kepada akun pengguna. Selain itu, bank perlu mengimplementasikan program edukasi yang komprehensif dan berkelanjutan untuk meningkatkan kesadaran dan pemahaman pengguna tentang pentingnya melaporkan insiden keamanan.

Penelitian ini telah memberikan wawasan penting akan perilaku keamanan informasi pengguna mobil banking. Namun penelitian ini memiliki keterbatasan dalam hal bias pemilihan sampel yang mungkin terjadi. Meskipun jumlah sampel cukup representatif, sampel mungkin belum mewakili keseluruhan populasi pengguna mobil banking yang lebih luas. Penelitian selanjutnya dapat dilakukan dengan ukuran sampel yang lebih luas dan mewakili semua kelompok demografis. Penelitan lain dapat juga dilakukan untuk mempelajari tren perilaku keamanan informasi dari waktu ke waktu. Penelitian lain yang mungkin menarik adalah mengeksplorasi pengaruh literasi digital terhadap perilaku keamanan informasi.

## Daftar Pustaka


[1]. S. Kim, D. Shin, and J. Lee, "The Adoption of Mobile Banking in Emerging Markets: A Cross-Country Study," Journal of Global Information Management, vol. 29, no. 3, pp. 1-23, 2021.

[2]. N. Yildirim and A. Varol, "A Research on Security Vulnerabilities in Online and Mobile Banking Systems," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, doi: 10.1109/ISDFS.2019.8757495.

[3]. S. Goel and R. Gupta, "Security Issues in Mobile Banking Applications: The Current State of Risks," International Journal of Information Management, vol. 50, pp. 456-468, 2020.

[4]. K. Parsons, E. Young, M. Butavicious, A. McCormac, M. Pattison, dan C. Jerram, "The Influence of organisational information security culture on cybersecurity decision making," *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 2, pp. 117-129, 2015.

[5]. Pricewaterhouse Coopers (PWC), "Turnaround and transformation in cybersecurity: key finding from The Global State of Information Security Survey 2016," 2015.

[6]. M. Hakami and M. Alshaikh, "Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study," *International Journal of Computer Science and Network Security*, vol. 22, no. 4, pp. 299-309, 2022.

[7]. I. Al-Shanfari, W. Yassin, N. Tabook, R. Ismail and A. Ismail, "Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, pp. 479-490, 2022.

[8]. V. Linkov, P. Zámečník, D. Havlíčková and C.-W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," *Frontiers in Psychology*, vol. 10, pp. 1-7, 2019.

[9]. G. K. Ajufo and A. Qutieshat, "An Examination of the Human Factors in Cybersecurity: Future Direction for Nigerian Banks," *Indonesian Journal of Information Systems (IJIS)*, vol. 6, no. 1, pp. 1-16, Aug. 2023

[10]. D. Shin and H. Kang, "Security Practices in Mobile Banking: User Awareness and Prevention Measures," Journal of Financial Services Marketing, vol. 26, no. 1, pp. 54-66, 2021.

[11]. K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," Computers & Security, vol. 66, pp. 40-51, May 2017, doi: 10.1016/j.cose.2017.01.004.

[12]. D. Iacobucci and A. Duhachek, "Advancing Alpha: Measuring Reliability With Confidence," Journal of Consumer Psychology, vol. 13, no. 4, pp. 478-487, 2003.
[13]. K.-c. Chang and C.-p. Wang, "Information systems resources and information security," *Information Systems Frontiers*, vol. 13, pp. 579-593, Apr. 2010. DOI: 10.1007/s10796-010-9232-6.
[14]. S. Lee, D. Lee, and M. Kang, "Factors Influencing User Behavior in Mobile Banking Security: An Empirical Study," Computers & Security, vol. 114, p. 102580, 2022.
[15]. J. Park, H. Jeong, and S. Kim, "Understanding the Influence of Security Awareness on Mobile Banking Use: A Comparative Study," Telematics and Informatics, vol. 57, p. 101508, 2021.