ANALISIS KESADARAN KEAMANAN DALAM PENGGUNAAN E-WALLET DI INDONESIA

Disusun Oleh:

N a m a : Muhammad Sulthon Alif
NIM : 17523069

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2020

HALAMAN PENGESAHAN DOSEN PEMBIMBING

ANALISIS KESADARAN KEAMANAN DALAM PENGGUNAAN E-WALLET DI INDONESIA

TUGAS AKHIR

Disusun Oleh:

N a m a : Muhammad Sulthon Alif

NIM : 17523069

Yogyakarta, 12 Desember 2020

Pembimbing

(Ahmad M. Raf'ie Pratama, S.T., M.I.T., Ph.D.)

HALAMAN PENGESAHAN DOSEN PENGUJI

ANALISIS KESADARAN KEAMANAN DALAM PENGGUNAAN E-WALLET DI INDONESIA

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 12 Januari 2021

Tim Penguji

Ahmad M. Raf'ie Pratama, S.T., M.I.T., Ph.D.

Anggota 1

Erika Ramadhani, S.T., M.Eng.

Anggota 2

Moh. Idris, S.Kom., M.Kom.

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Muhammad Sulthon Alif

NIM : 17523069

Tugas akhir dengan judul:

ANALISIS KESADARAN KEAMANAN DALAM PENGGUNAAN E-WALLET DI INDONESIA

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung resiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 12 Desember 2020

(Muhammad Sulthon Alif)

HALAMAN PERSEMBAHAN

Puji syukur saya panjatkan kepada Allah SWT atas rahmat dan karunianya tugas akhir ini dapat terselesaikan dengan baik dan lancar. Sholawat dan salam selalu terlimpahkan kepada junjungan Nabi Muhammad SAW. Terima kasih sebesar-besarnya kepada Allah SWT yang Maha Pengasih lagi Maha Penyayang karena tanpa seijin-Nya tugas akhir ini tidak mungkin terselesaikan dengan baik. Tak luput kepada Nabi Muhammad SAW, sebagai contoh teladan yang baik menjadi inspirasi untuk mengerjakan tugas akhir ini dengan maksimal dengan seluruh upaya yang ada agar menghasilkan yang terbaik oleh kemampuan saya.

Terima kasih kepada kedua orang tua saya yang telah mendukung perkuliahan saya sejak awal masuk sampai dengan selesainya tugas akhir ini, tanpa mereka saya bukanlah apa-apa. Sejak kecil saya dirawat dan dibesarkan dengan penuh kasih sayang yang tak terhingga hingga saat ini. Saya sadar tidak bisa mengembalikan semua hal yang telah diberikan orang tua kepada saya tetapi saya harapkan dengan ini menjadi sebuah awal agar orang tua saya merasa bahagia dan bangga karena telah membesarkan saya hingga saat ini.

Tak luput terima kasih kepada dosen pembimbing saya, karena atas bimbingan beliau selama saya mengerjakan tugas akhir ini dapat menghasilkan tugas akhir yang baik. Mulai dari konsultasi, gambaran, pengajuan judul, masukan dan saran, penyerahan draft, evaluasi, dan lain sebagainya dengan penjelasan dan arahan yang mudah dipahami.

Terima kasih juga kepada adik saya tercinta, dalam suka dan duka telah mendukung dan menghibur saya selama ini. Walaupun terkadang bertengkar, tetapi hal itu lah yang membuat kita selalu menjadi lebih dekat lagi. Semua hal tersebut akan selalu diingat hingga membekas di dalam hati sebagai sebuah kenangan yang indah.

Untuk teman dan sahabat saya, yang dari awal perkuliahan sangat dekat dan selalu menemani hari-hari berkuliah di kampus dengan canda tawa dan hiburan mereka yang sangat mengasyikkan. Terima kasih teman dan sahabat saya, Muhammad Asad Arifin Habibillah, Geraldy Yusuf Pralampita, Nunu Vadila, Dendy Surya Darmawan, Muhammad Aulia As Shidiq, serta Arga Arif Rahman yang telah membantu, menghibur, mendukung, dan menemani saya sejak awal berkuliah di Informatika hingga saat ini dalam suka dan duka. Kalian adalah teman sekaligus sahabat terbaik yang saya punya.

HALAMAN MOTO

وَاخْفِضْ لَهُمَا جَنَاحَ الذُّلِّ مِنَ الرَّحْمَةِ وَقُلْ رَبِّ ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا

“Dan katakanlah kepada keduanya perkataan yang mulia dan rendahkanlah dirimu terhadap keduanya dengan penuh kasih sayang. Dan katakanlah, “Wahai Rabb-ku sayangilah keduanya sebagaimana keduanya menyayangiku di waktu kecil”

Q.S. Al-Isra: 24

“Follow your passion. It will lead you to your purpose”

Oprah Winfrey

“Kerjakanlah dengan santai tanpa perlu terbebani, nikmatilah segala proses yang ada. Disitulah, makna dari kehidupan yang kita jalani”

Muhammad Sulthon Alif

KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, karena atas berkat rahmat dan karunia-Nya saya dapat menyelesaikan tugas akhir yang berjudul "Analisis Kesadaran Keamanan dalam Penggunaan E-Wallet di Indonesia". Sholawat dan salam dicurahkan kepada Muhammad SAW, yang telah menjadi sosok inspirasi suri tauladan yang baik.

Tugas Akhir ini dibuat untuk memenuhi persyaratan memperoleh gelar Sarjana Komputer di Universitas Islam Indonesia. Tugas akhir ini masih memiliki banyak kekurangan dikarenakan keterbatasan penulis tetapi diharapkan dapat bermanfaat dan menjadi acuan bagi penulis yang lain yang melakukan penelitian serupa.

Tidak lupa, dalam penulisan tugas akhir ini, saya menyampaikan banyak terima kasih kepada:

1. Kedua orang tua tersayang yang telah memberi semangat dan mendukung dalam penulisan tugas akhir ini.
2. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc. selaku Ketua Program Studi Informatika.
3. Bapak Ahmad M. Raf'ie Pratama, S.T., M.I.T., Ph.D. selaku dosen pembimbing tugas akhir yang sangat membantu selama proses penyusunan tugas akhir dari awal hingga akhir dengan memberi banyak arahan dan masukan kepada saya.
4. Bapak Andhik Budi Cahyono, S.T., M.T. selaku dosen pembimbing akademik yang membantu selama masa perkuliahan saya.
5. Seluruh dosen Program Studi Informatika yang banyak memberikan ilmu, pelajaran, pengalaman, serta nasihat selama saya berkuliah.
6. Teman-Teman yang telah mendukung dalam penulisan tugas akhir ini.

Saya berharap tugas akhir ini dapat bermanfaat dan berguna terutama menjadi acuan bagi orang-orang yang melakukan penelitian serupa dan bagi semua pihak serta dijadikan implikasi selanjutnya bagi mahasiswa.

Yogyakarta, 12 Desember 2020

(Muhammad Sulthon Alif)

SARI

Penggunaan E-Wallet di Indonesia terus meningkat dalam beberapa tahun terakhir. Di balik segala kemudahan dan kepraktisan dalam penggunaan yang ditawarkan, terdapat juga berbagai macam risiko keamanan yang mengintai penggunanya. Dikarenakan faktor manusia adalah salah satu unsur penting dalam keamanan siber dan informasi, kesadaran akan keamanan pun menjadi suatu hal yang sangat penting. Dengan menggunakan sumber data primer dari hasil survei daring terhadap 370 orang pengguna E-Wallet di Indonesia, penelitian ini mengukur tingkat *security awareness* dalam penggunaan E-Wallet di Indonesia dan melihat seberapa besar pengetahuan yang dimiliki pengguna serta bagaimana efeknya terhadap kebiasaan pengguna tersebut maupun perbedaan tingkat kesadaran keamanan berdasarkan faktor-faktor demografis penggunanya seperti jenis kelamin, usia, lokasi seperti kabupaten/kota maupun asal pulau, pendidikan terakhir, dan penghasilan bulanan. Dari hasil pengukuran berdasarkan model Kruger dan Kearney, secara umum tingkat kesadaran keamanan pengguna E-Wallet di Indonesia dapat dikatakan sudah cukup baik dengan beberapa peluang peningkatan di sisi pengetahuan, sikap, dan perilaku, utamanya yang terkait dengan area fokus PIN/Password, *software,* dan internet yang masih lebih rendah jika dibandingkan area fokus *hardware.* Selain itu, dari hasil analisis regresi linear berganda, penelitian ini juga menemukan penghasilan dan pendidikan sebagai dua faktor utama yang berpengaruh pada perbedaan tingkat kesadaran keamanan di kalangan pengguna E-Wallet di Indonesia. Hasil dari penelitian ini dapat dimanfaatkan untuk merancang berbagai jenis intervensi atau kebijakan khusus dalam rangka meningkatkan kesadaran keamanan di semua kalangan pengguna E-Wallet di Indonesia.

Kata kunci: kesadaran keamanan, *security awareness*, *e-wallet*, informasi, pembayaran.

GLOSARIUM

AHP	sebuah metode untuk memeringkat alternatif keputusan dan memilih yang terbaik dengan beberapa kriteria.
Bullet Proof	anti pembobolan atau anti pencurian.
Cashless	pembayaran tanpa menggunakan uang fisik atau non tunai.
Cyber Crime	tindak kejahatan melalui komputer dan jaringan internet.
E-Commerce	proses pembelian dan penjualan sebuah produk yang dilakukan secara elektronik.
E-Wallet	dompet digital yang digunakan untuk melakukan pembayaran transaksi jual beli secara non tunai.
Homogen	terdiri atas jenis, macam, sifat, watak, dan sebagainya yang sama.
Influential Cases	kasus apa pun yang secara signifikan mengubah nilai koefisien regresi setiap kali nilai tersebut dihapus dari analisis.
OLS	metode statistik analisis untuk memperkirakan atau menghitung hubungan antara satu atau lebih variabel independen dan variabel dependen.
OTP	kode yang dikirimkan melalui SMS kepada nomor pengguna untuk memvalidasi proses masuk ke dalam suatu akun.
Outliers	titik data yang sangat berbeda dengan titik data lainnya dalam suatu kumpulan data.
Phishing Attacks	metode penyerangan dengan mengumpulkan informasi pribadi target untuk memperoleh hak akses pada sejumlah aplikasi yang dimiliki target tersebut.
RStudio	IDE untuk pemrograman Bahasa R yang digunakan untuk komputasi statistik dan grafik.
Security Awareness	kesadaran keamanan yang dimiliki oleh setiap orang untuk melindungi segala informasi yang dimilikinya.
Social Engineering	teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan informasi pribadi, akses, atau barang berharga.
URL	alamat sumber yang bersifat unik pada sebuah web.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi *e-wallet* di Indonesia mengalami peningkatan yang pesat dari tahun ke tahun. Pada tahun 2014, Bank Indonesia mencanangkan program bernama Gerakan Nasional Non Tunai (GNNT) agar masyarakat Indonesia menjadi Less Cash Society (LCS) (Andika, Listiawati, Novitasari, & Vidyasari, 2019). Dengan adanya program tersebut, banyak perusahaan yang mulai membuat produk *e-wallet* di Indonesia seperti Gopay, OVO, LinkAja, Dana, E-Money, Jenius, dan lain sebagainya. Penggunaan *e-wallet* sendiri banyak macamnya seperti pembelian pulsa, pembayaran token listrik, pembayaran tagihan makan di restoran, pembayaran BPJS, pembayaran tagihan tv kabel, pembayaran tagihan belanja daring, hingga pembayaran pendidikan.

Tentu saja dengan semua penggunaan tersebut terdapat informasi-informasi yang berharga dan sensitif seperti uang atau finansial. Banyak masyarakat yang tidak sadar untuk mengamankan informasi-informasi tersebut secara pribadi dan malah memberitahu kepada orang lain. Dengan adanya hal tersebut maka akan menimbulkan sebuah ancaman terhadap para pengguna *e-wallet*. Beberapa kemungkinan kerentanan dari sisi pengguna meliputi kecerobohan ketika memvalidasi konten dalam email, pesan SMS, kunjungan ke tautan berupa *URL,* mengunduh lampiran, menggunakan koneksi Wi-Fi publik saat melakukan pembayaran, penggunaan *access point* palsu pada jaringan yang sama, penggunaan situs web palsu, hingga ketiadaan minimal standar peraturan untuk menginstal aplikasi dan berkas yang tidak terpercaya pada perangkat (Bosamia & Patel, 2019).

Di Indonesia sendiri banyak kasus penipuan yang sering terjadi dikarenakan pengguna tidak paham dengan keamanan data yang harusnya mereka jaga dan tidak disebarkan secara cuma-cuma seperti kode OTP (One-Time Password). Salah satu kasus yang terjadi dialami oleh artis Aura Kasih pada tahun 2019. Aura Kasih mengaku kehilangan uang Rp 11 juta dari akun Gopay miliknya. Ia pun langsung melaporkan masalah ini ke kantor ojek *online* yang bersangkutan, dalam hal ini Gojek (Iskandar, n.d.). “Kami sangat menyesalkan kasus penipuan atas nama Gojek yang menimpa Aura Kasih. Penipuan berbasis *social engineering* seperti ini sudah ada dari dulu, seperti halnya penipuan 'mama minta pulsa',” kata Kristy Nelwan, VP Corporate Communications Gojek (Iskandar, n.d.).

Oleh sebab itu, perlu adanya kesadaran keamanan informasi dari masyarakat pengguna E-Wallet agar informasi pribadi terjaga. Pentingnya pemahaman tentang keamanan informasi demi menjaga data privasi dan meminimalisir tindak kejahatan yang sekarang marak terjadi seperti *Cyber Crime* atau kejahatan dunia maya dan masalah keamanan informasi lainnya (Batmetan, Kariso, Moningkey, & Tumembow, 2018). Pentingnya meningkatkan kesadaran mahasiswa maupun masyarakat tentang keamanan informasi berguna untuk menghindari resiko kerugian seperti kebocoran informasi, penyalahgunaan data pribadi, pemalsuan identitas, dan hal-hal yang dapat menimbulkan kerugian terhadap pengakses layanan publik (Batmetan et al., 2018).

1.2 Rumusan Masalah

Dari penjelasan latar belakang yang telah disampaikan sebelumnya, maka yang menjadi rumusan masalah pada tugas akhir ini adalah sebagai berikut:

a. Seberapa besar pengetahuan tentang keamanan di kalangan pengguna *e-wallet* di Indonesia?
b. Bagaimana tingkat kesadaran keamanan di kalangan pengguna *e-wallet* di Indonesia?
c. Bagaimana dampak pengetahuan dan kesadaran akan keamanan tersebut dalam kebiasaan penggunaan *e-wallet* di Indonesia?
d. Apakah ada perbedaan tingkat pengetahuan dan kesadaran akan keamanan, serta kebiasaan penggunaan *e-wallet* berdasarkan faktor demografis seperti jenis kelamin, usia, lokasi seperti kabupaten/kota maupun asal pulau, pendidikan terakhir, dan penghasilan bulanan di Indonesia?

1.3 Tujuan Penelitian

Menganalisis dan mengukur seberapa besar pengetahuan tentang keamanan, bagaimana tingkat kesadaran keamanan, bagaimana dampak pengetahuan dan kesadaran akan keamanan tersebut dalam kebiasaan penggunaan, serta apakah ada perbedaan tingkat pengetahuan dan kesadaran akan keamanan, serta kebiasaan penggunaan *e-wallet* berdasarkan faktor demografis seperti jenis kelamin, usia, lokasi seperti kabupaten/kota maupun asal pulau, pendidikan terakhir, dan penghasilan bulanan di Indonesia melalui uji statistik untuk menjawab masing-masing rumusan masalah di atas.

1.4 Lingkup Penelitian

Ruang lingkup penelitian ini akan dibatasi pada beberapa hal diantaranya:

a. Pengambilan data dilakukan melalui survei daring via Google Forms yang akan disebar di beberapa platform media sosial.
b. Kriteria responden untuk penelitian ini yaitu pengguna yang menggunakan *e-wallet* se-Indonesia.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini diantaranya menjadi sebuah sumber acuan baru bagi para peneliti yang akan melakukan penelitian seputar kesadaran keamanan pengguna *e-wallet* di Indonesia baik dari dalam kampus maupun luar kampus dan menjadi sebuah acuan atau patokan seberapa besar pengetahuan tentang keamanan, bagaimana tingkat kesadaran keamanan, bagaimana dampak pengetahuan dan kesadaran akan keamanan tersebut dalam kebiasaan, apakah ada perbedaan tingkat pengetahuan dan kesadaran akan keamanan, serta kebiasaan penggunaan *e-wallet* berdasarkan faktor demografis seperti jenis kelamin, usia, lokasi seperti kabupaten/kota maupun asal pulau, pendidikan terakhir, dan penghasilan bulanan dari kalangan pengguna *e-wallet* di Indonesia.

BAB II
KAJIAN PUSTAKA

2.1 Kajian Pustaka

2.1.1 *Security Awareness*

Keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi (Whitman & Mattord, 2011). Terdapat empat definisi privasi informasi yaitu privasi sebagai hak asasi manusia, privasi sebagai komoditas, privasi sebagai keadaan akses terbatas, dan privasi sebagai kemampuan untuk mengendalikan informasi tentang diri sendiri (Jeff Smith, Dinev, & Xu, 2011).

Sementara keamanan informasi umumnya berfokus pada perlindungan dalam hal kerahasiaan, integritas dan ketersediaan informasi, kesadaran keamanan informasi berkaitan dengan penggunaan program kesadaran keamanan untuk menciptakan dan memelihara perilaku keamanan yang positif sebagai elemen penting dalam lingkungan keamanan informasi yang efektif (Kruger & Kearney, 2006). Menurut (Hansche, 2001) tujuan dari program kesadaran keamanan adalah untuk meningkatkan pentingnya keamanan sistem informasi dan kemungkinan efek negatif dari pelanggaran atau kegagalan suatu keamanan.

Dengan segala informasi dan privasi diantara masing-masing individu tersebut, maka semua orang harus memiliki kesadaran dalam melindungi informasi pribadi dengan sebaik mungkin. Salah satu faktor yang menjadi pemicu terjadinya pelanggaran keamanan informasi dan privasi adalah karena pengguna *smartphone* memiliki kesadaran yang tidak memadai dalam menggunakan *smartphone* dengan aman, beberapa dari mereka memiliki pengetahuan yang cukup memadai dalam penggunaan *smartphone* tetapi mereka tidak menerapkannya dengan baik (Al-Shehri, 2012). Dengan begitu, *security awareness* atau kesadaran keamanan sangat perlu dimiliki oleh setiap orang untuk menghindari pelanggaran keamanan. *Security Awareness* adalah kontrol/aturan yang dirancang untuk mengurangi insiden pelanggaran terhadap keamanan informasi, akibat dari kelalaian maupun tindakan yang telah direncanakan (Whitman & Mattord, 2011).

Security awareness sendiri tentu saja memiliki banyak cakupan bahasan, salah satunya *Information Security Awareness* atau ISA. ISA mengacu pada sejauh mana karyawan memahami pentingnya kebijakan, aturan, dan pedoman keamanan informasi pada organisasi

mereka dan sejauh mana mereka berperilaku sesuai dengan kebijakan, aturan, dan pedoman ini (Siponen, 2000). Adapun banyak faktor yang mempengaruhi seseorang dalam menerapkan kesadaran keamanan dengan semestinya seperti kebiasaan atau karakteristik sifat dan perilaku orang itu sendiri. Sampai saat ini, aspek manusia dari penelitian keamanan informasi biasanya berfokus pada pemahaman kerentanan manusia di tingkat individu dengan mengeksplorasi karakteristik spesifik yang mungkin berhubungan dan mempengaruhi perilaku keamanan informasi (McCormac et al., 2017).

Banyak sekali yang bisa dilakukan untuk memunculkan kesadaran keamanan seperti seminar ataupun pelatihan yang berkaitan dengan kesadaran keamanan. Menurut (Wilson & Hash, 2003) kesadaran bukanlah pelatihan tetapi tujuan dari presentasi kesadaran hanyalah untuk memusatkan perhatian pada keamanan yang dimaksudkan untuk memungkinkan individu mengenali masalah keamanan TI dan meresponnya dengan sesuai. Program kesadaran dan pelatihan bisa efektif jika materinya menarik, terkini, dan cukup sederhana untuk diikuti (Bada, Sasse, & Nurse, n.d.). Setiap presentasi yang 'terasa' impersonal dan terlalu umum untuk diterapkan pada audien yang dituju akan diperlakukan oleh pengguna hanya sebagai sesi wajib lainnya (Wilson & Hash, 2003).

Dengan banyaknya penjelasan terkait hal tersebut dan menjadikan semua itu sangat penting di era sekarang ini menjadi sebuah pertimbangan mengapa penelitian yang saya lakukan berfokus pada *Security Awareness* atau Kesadaran Keamanan.

2.1.2 E-Wallet

Pada tahun 2014, Bank Indonesia mencanangkan program bernama Gerakan Nasional Non Tunai (GNNT) agar masyarakat Indonesia menjadi Less Cash Society (LCS) (Andika et al., 2019). *E-wallet* sendiri memiliki banyak sebutan seperti *E-Money* (Electronic Money), *Mobile Payment*, *Mobile Wallet*, dan lain sebagainya yang pada dasarnya memiliki konsep yang sama yaitu untuk melakukan transaksi nontunai. Alat pembayaran nontunai adalah alat pembayaran yang digunakan untuk membeli barang atau jasa berupa uang yang tidak dibayarkan secara tunai (Andika et al., 2019). Sistem pembayaran elektronik terdiri dari kartu kredit *online* transaksi, dompet elektronik (*e-wallet*), uang tunai elektronik (*e-cash*), sistem nilai tersimpan *online*, sistem saldo akumulasi digital, sistem pembayaran pengecekan digital dan sistem pembayaran nirkabel (Laudon, Kenneth C., & Traver, 2011). Dengan perkembangan teknologi yang semakin canggih, kini telah dikenal *electronic money* (*e-money*) atau uang elektronik (Andika et al., 2019).

Dompet elektronik (*e-wallet*) sama seperti dompet fisik, digunakan untuk menyimpan informasi seperti nomor kartu kredit, *e-cash*, identitas pemilik, informasi kontak, informasi pengiriman atau penagihan termasuk alamat pelanggan dan informasi lain yang digunakan pada saat pembayaran di situs *e-commerce* (Junadi & Sfenrianto, 2015). Uang elektronik (*e-cash*) adalah istilah yang digunakan untuk menggambarkan nilai yang disimpan dan dapat ditukar melalui sistem yang dibuat oleh entitas (bukan pemerintah) tanpa menggunakan dokumen kertas atau koin, tetapi dapat digunakan sebagai pengganti mata uang yang dikeluarkan oleh pemerintah (Schneider, 2011). Konsep dasar *e-cash* adalah proses pembayaran melalui internet melalui token unik yang sudah diautentikasi yang merepresentasikan uang dari konsumen ke *merchant* (Junadi & Sfenrianto, 2015). Konsumen akan melakukan deposit sejumlah uang atau kartu kredit, kemudian bank akan memberikan token (nomor unik terenkripsi) dalam beberapa denominasi uang untuk digunakan berbelanja di situs merchant (Junadi & Sfenrianto, 2015). Merchant akan menukarkan tokennya kembali ke bank untuk mendapatkan uang yang sebenarnya (Laudon, Kenneth C., & Traver, 2011).

E-wallet digunakan untuk berbagai macam transaksi secara nontunai atau tanpa menggunakan uang fisik seperti yang biasa kita gunakan. Salah satu transaksi tersebut adalah berbelanja via daring melalui berbagai macam *e-commerce* yang ada di Indonesia. Menurut (iPrice Group, 2020) pada Q2 2020, lima *e-commerce* yang memiliki pengunjung terbanyak secara berurutan adalah Shopee dengan pengunjung sekitar 93 juta orang, Tokopedia dengan pengunjung sekitar 86 juta orang, Bukalapak dengan pengunjung sekitar 35 juta orang, Lazada dengan pengunjung sekitar 22 juta orang, dan Blibli dengan pengunjung sekitar 18 juta orang. Dengan banyaknya pengunjung pada *e-commerce* tersebut akan menyebabkan banyaknya pula pengguna *e-wallet* untuk melakukan transaksi berbelanja daring melalui berbagai macam e-commerce dikarenakan beberapa *e-commerce* yang bekerja sama dengan *e-wallet* tersebut. Misalnya Tokopedia, *e-commerce* ini menjalin kerja sama dengan perusahaan *e-wallet* OVO untuk mempermudah pembayaran belanja pada Tokopedia tersebut.

Menurut (iPrice Group & App Annie, 2019) Q2 2019, sepuluh aplikasi *e-wallet* yang paling populer di Indonesia secara berurutan adalah Gojek (Gopay), OVO, Dana, LinkAja, iSaku, Jenius, Go Mobile by CIMB, Paytren, Sakuku, dan DOKU. *E-wallet* adalah sebuah sistem yang menyimpan data konsumen untuk memudahkan pengambilan transaksi pembelian *online* (Kanimozhi. G, 2017). Untuk membatalkan transaksi, maka harus mengisi formulir transaksi *e-retail* yang dijadikan alasan, dengan layanan *e-wallet*, hal ini dapat mengurangi ketidaknyamanan bagi konsumen (Kanimozhi. G, 2017). *Mobile wallet* terus tumbuh dan

memengaruhi banyak faktor seperti peningkatan pengembangan, penetrasi seluler, inklusi keuangan, lebih nyaman, lebih cepat, dan lebih ekonomis (Bosamia & Patel, 2019).

Tetapi tentu saja *e-wallet* tidak luput dari ancaman yang mengintai diluar sana. *Mobile Wallet* memiliki beberapa ancaman seperti *Phishing attacks, Social engineering, Unintentional installation of rogue and malware applications, dan Mobile Operating System Access Permissions* (Bosamia & Patel, 2019). Dengan adanya sebuah pernyataan bahwa *e-wallet* terus tumbuh dan memengaruhi banyak faktor terutama keuangan, maka *e-wallet* bisa menjadi sebuah topik penelitian yang menarik untuk diangkat.

2.1.3 Risiko Keamanan melalui OTP (*One-Time Password*)

Pada *e-wallet* yang sering kita pakai khususnya di Indonesia, ada beberapa sistem keamanan yang dirancang untuk mengamankan aplikasi *e-wallet* tersebut salah satunya *One-Time Password* atau OTP. Kasus pembobolan dompet digital yang terjadi di Indonesia justru diakibatkan dari sisi pengguna yang mudah dimanipulasi karena sistem pada dompet digital yang berpengalaman biasanya sudah *bullet proof* atau anti bobol (Rudi Adianto, 2020). Menurut (Rudi Adianto, 2020) jika dari segi teknisnya sudah *bullet proof,* maka sisi manusianya bisa jadi target sebab mata rantai yang paling lemah pada suatu sistem adalah elemen manusianya dan yang mudah dimanipulasi. Lanjut menurut (Rudi Adianto, 2020) di Indonesia peretasan tidak sampai harus peretas punya *skill* teknikal tapi murni *social engineering* bagaimana menggunakan satu dan lain cara agar korban memberikan kode OTP.

Dari pandangan pakar IT bisa dilihat bahwa pembobolan *e-wallet* disebabkan karena kurangnya kesadaran dan pemahaman dalam menggunakan aplikasi itu. Penipu ini cenderung menargetkan untuk mendapat kode *One-Time Password* (OTP) dari korban untuk mengambil hak akses pada *e-wallet* yang korban gunakan. Namun pada sejumlah kejadian, korban cenderung diperdaya karena ketidaktahuan informasi, misalnya, tentang kode *Call Forwarding* ini yang dialami oleh Maia atau korban masih belum paham bahwa OTP adalah kode penting yang tak boleh diserahkan kepada siapa pun saat bertransaksi di aplikasi (“Waspada! Akun Dompet Digital Rawan Dibobol Hacker,” 2020).

Menurut Country Manager Indonesia CashShield, Kevin Onggo, angka penipuan (*fraud*) di sektor keuangan terbilang tinggi mulai kasus kartu kredit hingga dompet digital. Menurut Kevin Onggo, di Indonesia mayoritas target penipuan adalah pengguna *e-wallet*. Misalnya, penipuan lewat modus permintaan *one-time password* (OTP) ke pengguna dompet digital tersebut (“Awas! Penjahat di Indonesia Incar Dompet Digital,” 2019). Ini membuat adanya

kerentanan pada dompet digital atau *e-wallet* melalui kode OTP yang mana mesti dijaga kerahasiannya dan tidak dibagikan ke pihak manapun untuk menghindari penipuan atau pembobolan *e-wallet*. Kesadaran dan pemahaman akan fitur keamanan tersebut perlu dimiliki oleh setiap orang untuk menghindari risiko pembobolan yang bisa saja terjadi oleh oknum yang tidak bertanggung jawab.

Pada dasarnya OTP digunakan untuk transaksi *online* dan kegiatan perbankan digital sejenisnya yang berisikan 4 sampai 6 angka acak yang dikirimkan ke nomor *smartphone* yang kita gunakan dan didaftarkan pada aplikasi *e-wallet* tersebut untuk memastikan pengguna yang masuk merupakan pemiliki akun tersebut yang sah. Hal ini seperti yang sudah dibahas di atas banyak dimanfaatkan oleh berbagai oknum untuk mendapatkan hak akses *e-wallet* kita untuk melakukan pembobolan.

2.1.4 Risiko Keamanan melalui Phishing Attacks

Selain dari OTP, ada pula risiko keamanan melalui *Phishing Attacks* yang dilakukan oleh penipu atau oknum tertentu untuk membobol *e-wallet* miliki kita. *Phishing* dan *Pharming* adalah metode yang digunakan untuk mengumpulkan informasi pribadi oleh penyamar sebagai organisasi yang dapat dipercaya (Urs, 2015). Biasanya penyerang mengirim *email* yang tampaknya dari perusahaan kartu kredit atau lembaga keuangan terkemuka yang meminta informasi akun, seringkali menunjukkan bahwa ada masalah (Urs, 2015). Ketika pengguna menanggapi dengan informasi yang diminta, penyerang dapat menggunakannya untuk mendapatkan akses ke akun tersebut (Vrîncianu & Popa, 2010). Serangan *phishing* juga dipakai untuk mencuri detail login pengguna dan data pribadi, selanjutnya penjahat bisa mengakses akun dompet digital ("NEWS : Tiga Serangan yang Dipakai untuk Bobol Dompet Digital," 2020).

Dari data yang dikumpulkan oleh The International Criminal Police (Interpol) pada semester I tahun lalu, lembaga ini mencatat Indonesia adalah target *phising* tertinggi di Asia Tenggara dengan 31,07% upaya ("Kenali Maraknya Penipuan Online saat Pandemi - Analisis Data Katadata," 2020). Menurut Data Pusat Operasi Kemananan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber sejak 1 Januari-12 April 2020 yang puncaknya terjadi pada tanggal 12 Maret 2020 yang mencapai 3.344.470 serangan per hari. Dari data ini didapat tingginya upaya phishing yang dilakukan oleh sejumlah pihak. Selanjutnya dari Data Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri sepanjang Januari-September 2020 yang menerima laporan

sejumlah kasus kejahatan siber berhubungan dengan phishing seperti penipuan *online* (649 laporan), akses ilegal (138 laporan), manipulasi data (71), dan pencurian data/identitas (39).

Dari data-data tersebut, banyak sekali upaya *phishing* yang dilakukan dan dapat membahayakan pengguna dompet digital atau *e-wallet* jikalau pengguna terkena phishing tersebut. Mulai dari data pribadi yang dicuri, nominal uang yang ada, akses ke berbagai aplikasi yang tersambung dan lain sebagainya. Menurut data International Telecommunication Union, lebih dari 90% negara pun kurang memperhatikan pentingnya keamanan siber, termasuk Indonesia. Sedangkan laporan Global Cybersecurity Index 2018 menempatkan Indonesia di peringkat 41 dari 175 negara yang dengan kata lain masih jauh dari kata aman.

2.2 Landasan Teori

2.2.1 Model Kruger dan Kearney

Metodologi ini digunakan untuk mengembangkan alat ukur yang didasarkan pada teknik yang dipinjam dari bidang psikologi sosial yang mengusulkan bahwa kecenderungan yang dipelajari untuk merespons dengan cara yang menguntungkan atau tidak menguntungkan untuk objek tertentu memiliki tiga komponen yaitu pengaruh, perilaku dan kognisi (Kruger & Kearney, 2006). Komponen pengaruh meliputi emosi positif dan negatif seseorang tentang sesuatu, komponen perilaku terdiri atas niat untuk bertindak dengan cara tertentu sedangkan komponen kognisi mengacu pada keyakinan dan pemikiran yang dipegang seseorang tentang suatu objek (Feldman, 1999; Michener & Delamater, 1994). Ketiga komponen ini digunakan sebagai dasar dan model yang dikembangkan pada tiga dimensi ekuivalen yaitu apa yang diketahui seseorang (pengetahuan); bagaimana perasaan mereka tentang topik (sikap); dan apa yang mereka lakukan (perilaku) (Kruger & Kearney, 2006).

Sebagai klasifikasi pertama dari apa yang harus diukur, itu diputuskan untuk mengukur tiga dimensi yaitu *knowledge* (apa yang anda ketahui), *attitude* (apa yang anda pikirkan) dan *behavior* (apa yang anda lakukan) (Kruger & Kearney, 2006). Masing-masing dari dimensi tersebut kemudian dibagi menjadi enam area fokus seperti yang dibahas dan menjadi dasar program kesadaran (Kruger & Kearney, 2006). Untuk mendapatkan nilai *knowledge*, *attitude,* dan *behavior,* maka dilakukan dengan memberi sejumlah pertanyaan kepada responden melalui sebuah kuesioner. Beberapa pertanyaan yang dijawab di skala dengan 3 poin benar, tidak tahu, dan salah (dimensi *attitude* dan *knowledge*), sementara yang lain hanya memerlukan respon benar dan salah saja (dimensi *behavior*) (Kencana Sari & Candiwan, 2014).

Selanjutnya, perlu dilakukan pembobotan pada dimensi dan area fokus. Pembobotan kesadaran ditentukan menggunakan *Analytical Hierarchy Process* (AHP) (Kencana Sari & Candiwan, 2014). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi subyektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen (Akraman, Candiwan, & Priyadi, 2018). Setiap dimensi akan memiliki bobot masing-masing yang digunakan dalam perhitungan kesadaran atau *awareness* nantinya.

2.2.2 Google Forms, Google Sheets, dan Microsoft Excel

Google Forms merupakan alat yang sangat berguna untuk memfasilitasi koleksi data dan analisis (Hsu & Wang, 2017). Google Forms (dilihat dari *Resources*) adalah sistem gratis untuk membuat dokumen berbasis *cloud* yang memungkinkan pengguna membuat pengumpulan data secara kolaboratif (Hsu & Wang, 2017). Ia memiliki fungsi spreadsheet yang memungkinkan pengguna untuk menganalisis data dalam format multimodal (Hsu & Wang, 2017). Selain untuk mengumpulkan data, Google Forms pun dapat menampilkan data yang telah terkumpul dalam bentuk grafik pie atau batang dari setiap pertanyaan pada kuesioner. Pada penelitian ini, Google Forms digunakan untuk membuat kuesioner yang kemudian disebarkan di beberapa *platform* soial media seperti WhatsApp, Telegram, Instagram, Twitter, dan Facebook. Melalui kuesioner yang dibuat di Google Forms, responden yang telah mengisi akan langsung diterima datanya dan bisa dibuka melalui Google Sheet atau di download terlebih dahulu dalam format xlsx apabila hendak dibuka di Microsoft Excel.

Google Sheets adalah program *spreadsheet* berbasis *cloud* yang dimiliki oleh Google dan memiliki banyak fungsi yang sama dengan MS Excel (Kunicki et al., 2019). Program ini tersedia untuk setiap pengguna yang mendaftar pada akun Google (Kunicki et al., 2019). Pengguna dapat dengan mudah mengunggah atau memasukkan data kemudian menulis kode untuk menganalisis data (Kunicki et al., 2019). Setiap data yang dimasukkan ke dalam Google Sheets disimpan di *cloud server* yaitu Google Drive yang memungkinkan aksesibilitas setiap saat ketika seseorang masuk ke akun Google mereka tanpa terikat dengan lokasi atau komputer (Kunicki et al., 2019). Tetapi ketika menggunakan Google Sheets harus selalu ingat untuk tetap terhubung dengan jaringan internet untuk menyimpan kemajuan pada data yang kita olah. Google Sheets digunakan untuk menampung data yang dikumpulkan dari kuesioner yang bisa diolah langsung ketika pengumpulan data dari responden sudah dirasa cukup untuk penelitian ini.

Microsoft Excel adalah aplikasi *spreadsheet* serbaguna yang banyak digunakan oleh dokter, ilmuwan biomedis dan siswa (Slezak, 2014). Peneliti sering merekam peristiwa, hitungan dan proporsi untuk menyediakan bukti kepada asosiasi antara karakteristik populasi tertentu, misalnya antara faktor risiko yang mungkin dan penyakit (Slezak, 2014). Microsoft Excel menyediakan alat bantu untuk analisis statistic yang sederhana seperti *t-tests*, *F-test*, ANOVA, korelasi dan regresi *Ordinary Least Squares* (OLS) (Slezak, 2014). Microsoft Excel juga memungkinkan representasi yang mudah dari data kategorikal dan membuat klasifikasi silang tabel dari data mentah (Slezak, 2014). Untuk melakukan analisis pada penelitian ini, peneliti lebih sering menggunakan Microsoft Excel dikarenakan bisa digunakan kapan saja dan tidak bergantung pada sinyal jaringan internet. Selain itu, pemakaiannya yang cukup mudah dan lebih familiar untuk peneliti membuatnya menjadi program utama untuk menganalisis data yang dikumpulkan dan melakukan pembersihan data.

2.2.3 Analisis Regresi Linear Berganda

Regresi linear berganda (multiple linear regression) adalah model regresi linear dengan 1 variabel dependen kontinu beserta k (dua atau lebih) variabel independen kontinu dan/atau kategorik (Harlan, 2018). Teknik regresi linear (garis lurus) berganda digunakan ketika kita ingin menganalisis pengaruh maupun memprediksi k variabel bebas (*independent variable*), yaitu X1, X2. . ., Xk dengan satu variabel terikat (*dependent variable*), yaitu Y' (Setiawan, 2017). Selanjutnya, perlu dilakukan pembobotan pada dimensi dan area fokus. Regresi Linear berganda dibagi menjadi beberapa macam yaitu regresi linear berganda dengan prediktor kontinu, regresi linear berganda dengan prediktor kategorik non biner, dan regresi linear berganda dengan interaksi.

2.2.4 Bahasa R dan IDE RStudio

R merupakan Bahasa pemrograman statistika yang dapat digunakan untuk analisis dan manipulasi data statistika (pemodelan statistika), dan grafik (Gio & Effendie, 2018). R diciptakan oleh Ross Ihaka dan Robert Gentleman dari departemen statistika, di Universitas Auckland, New Zealand (Gio & Effendie, 2018). R tersedia beberapa sistem operasi seperti Windows, Mac OS X, dan Linux yang dapat diunduh di website *https://cran.r-project.org/*. Setelah menginstal R dan dijalankan maka akan muncul sebuah tampilan editor dasar R. Tampilan tersebut pada sistem operasi Windows disebut *RGui*, sementara pada Mac OS X disebut *R.app*.

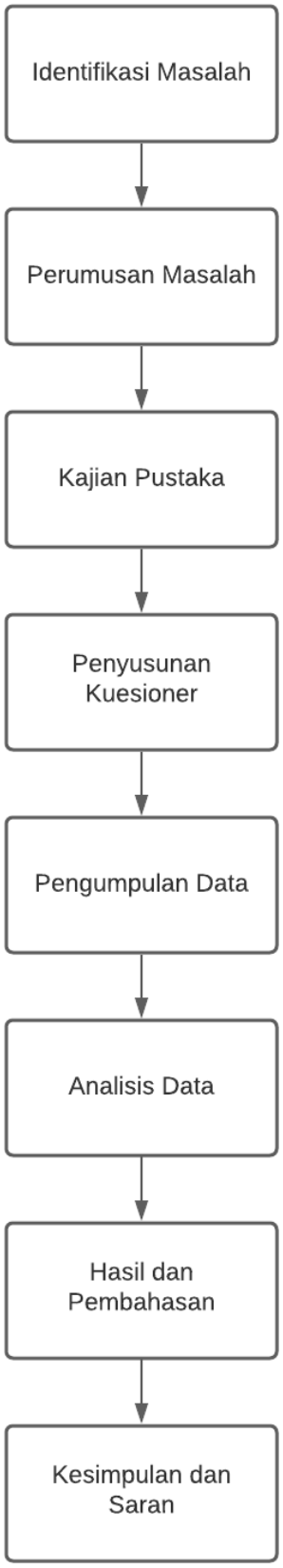
Untuk membantu pemrograman menggunakan Bahasa R dapat dibantu melalui fasilitas atau *package* yang disediakan RStudio. Rstudio adalah *Integrated Development Environment* (IDE) yang tersedia dari server CRAN (*Comprehensive R Archive Network*) untuk memudahkan analisis dan manipulasi data serta grafik dari data yang akan diolah. Rstudio telah menyediakan hampir semua fitur yang diinginkan untuk sebuah IDE dengan cara yang baru, membuatnya lebih mudah dan lebih produktif untuk menggunakan R (Vernazi, 2011). RStudio menyediakan banyak kenyamanan dan kemudahan dalam menggunakannya untuk mengatur *packages, workspaces, files,* dan lainnya (Vernazi, 2011). Rstudio merupakan *open source project* dengan pengembangan alat yang luar biasa supaya dapat membantu praktik dan teknik yang dibutuhkan dalam menciptakan analisis yang berkualitas (Vernazi, 2011).

BAB III
METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Terdapat dua jenis penelitian yaitu penelitian kualitatif dan kuantitatif. Menurut (Suliyanto, 2018) tujuan penelitian kualitatif yaitu untuk mendapatkan pemahaman kualitatif terhadap suatu fenomena sedangkan tujuan penelitian kuantitatif yaitu untuk mengukur data dan melakukan generalisasi hasil dari sampel ke populasi. Pada tugas akhir ini, penelitian yang dilakukan adalah jenis penelitian kuantitatif di mana data yang dikumpulkan akan dihitung dan diukur melalui uji statistik untuk menjawab masing-masing rumusan masalah. Data yang digunakan merupakan kumpulan hasil jawaban dari responden yang menjawab melalui kuesioner yang disebar di beberapa platform sosial media seperti WhatsApp, Telegram, Instagram, Twitter, dan Facebook. Kemudian, dilanjutkan kepada proses analisis statistik dari data yang telah dikumpulkan untuk mendapatkan hasil skor kesadaran keamanan pengguna E-Wallet yang ada di Indonesia.

Dalam penelitian ini, ada beberapa tahapan yang dilakukan mulai dari identifikasi masalah, perumusan masalah, kajian pustaka, penyusunan kuesioner, pengumpulan data, analisis data, hasil dan pembahasan, dan yang terakhir kesimpulan dan saran. Lalu adapun sampel yang digunakan merupakan bagian kecil dari populasi penelitian yang dilakukan dikarenakan populasi yang begitu luas yang mencakup seluruh Indonesia. Alur penelitian yang dilakukan dan bagian sampel dari populasi dapat dilihat pada Gambar 3.1 dan 3.2 di bawah ini.



Gambar 3.1 Diagram Alur Penelitian

Gambar 3.2 Diagram Venn Antara Populasi dan Sampel

3.2 Pengumpulan Data

Untuk melakukan sebuah penelitian, maka perlu dilakukan terlebih dahulu analisis dari berbagai aspek seperti pengumpulan data. Di dalam pengumpulan data tersebut terbagi menjadi beberapa bagian yaitu cara pengumpulan data, waktu pengumpulan data, populasi, dan sampel. Kemudian, teknik *sampling* yang digunakan untuk pengumpulan data penelitian ini merupakan gabungan dari *purposive sampling* dan *snowball sampling.*

Teknik *purposive sampling* juga disebut *judgement sampling*, adalah pilihan yang disengaja dari partisipan karena kualitas yang dimiliki partisipan (Etikan, 2016b). Teknik *purposive sampling* bisa artikan pula teknik pengambilan data sesuai dengan kriteria dan kebutuhan pada suatu penelitian. Pada penelitian ini, karena tujuannya adalah mencari nilai kesadaran keamanan pengguna *e-wallet* di Indonesia, maka pengumpulan datanya pun disesuaikan dengan kriteria responden yang dibutuhkan yaitu kalangan pengguna *e-wallet* di Indonesia.

Snowball sampling atau *chain referral sampling* dari populasi yang tersembunyi dimulai dengan *convenience sample* dari subjek awal, karena jika sampel acak dapat diambil, populasi tidak akan dibatasi sebagai tersembunyi (Etikan, 2016a). Subjek awal ini berfungsi sebagai "benih" di mana subjek gelombang 1 direkrut kemudian subjek gelombang 1 secara bergantian merekrut subjek gelombang 2 dan sampel sebagai konsekuensinya mengembang gelombang

demi gelombang seperti bola salju yang membesar saat berguling menuruni bukit (Heckathorn, 2011). Salah satu bentuk pengambilan sampel non-probabilitas yang paling terkenal adalah metode *snowball sampling*, yang sangat cocok jika populasi yang dibutuhkan sulit dijangkau dan sulit untuk disusun daftar populasinya oleh peneliti (Etikan, 2016a). Teknik *snowball sampling* bisa didefinisikan sebagai sebuah teknik pengambilan sampel data yang bersifat berantai, misal kuesioner disebar ke orang A kemudian dari orang A disebar lagi ke orang B dan C lalu disebar lagi ke orang D, E, F, dan seterusnya.

3.2.1 Cara Pengumpulan Data

Jika dilihat dari cara pengumpulannya, maka pengumpulan data dapat dilakukan dengan cara seperti tes, angket/kuesioner, wawancara, observasi/pengamatan, dokumen, dan photo/film (Barlian, 2016). Dari beberapa cara di atas, saya memilih menggunakan kuesioner dikarenakan butuh banyak data responden. Angket/kuesioner lebih popular dalam penelitian dibandingkan dari jenis instrument yang lain karena dengan menggunakan cara ini dapat dikumpulkan informasi/data yang lebih banyak dalam waktu relatif singkat serta biaya yang lebih rendah (Barlian, 2016).

Dalam penelitian ini, pengumpulan data dilakukan melalui kuesioner via Google Forms yang akan disebar di beberapa platform sosial media seperti WhatsApp, Telegram, Instagram, Twitter, dan Facebook yang mana para responden akan mengisi jawaban untuk masing-masing pernyataan yang terdapat pada form tersebut sampai mencapai jumlah target responden tertentu yang akan ditentukan. Kemudian, data responden tersebut dilakukan pembersihan data untuk menghindari duplikasi ataupun responden yang tidak sesuai dengan kriteria penelitian ini.

3.2.2 Waktu Pengumpulan Data

Dari segi waktu, pengumpulan data bisa dibagi menjadi 2 yaitu *Longitudinal* dan *Cross Section*. Penelitian dengan pendekatan *longitudinal* (pendekatan bujur) adalah penelitian yang meneliti perkembangan sesuatu aspek atau sesuatu hal dalam seluruh periode waktu, atau tahapan perkembangan yang cukup panjang (Siyoto & Sodik, 2015). Penelitian dengan pendekatan *cross section* adalah penelitian dalam satu tahapan atau satu periode waktu, hanya meneliti perkembangan dalam tahapan-tahapan tertentu saja (Siyoto & Sodik, 2015).

Menurut waktu pengumpulan, data ini akan termasuk ke dalam *Cross Section/Insidentil* yaitu data akan dikumpulkan dalam suatu rentang waktu tertentu. Dalam penelitian ini waktu

yang diperlukan untuk mengumpulkan data dari responden adalah 14 hari kalender, dimulai dari tanggal 22 September 2020 sampai 6 Oktober 2020.

3.2.3 Populasi

Populasi adalah merupakan wilayah generalisasi yang terdiri dari obyek/subyek yang memiliki kuantitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya (Siyoto & Sodik, 2015). Populasi tak hanya meliputi jumlah obyek yang diteliti, akan tetapi meliputi semua karakteristik serta sifat- sifat yang dimiliki obyek tersebut (Siyoto & Sodik, 2015).

Dalam penelitian ini, populasi dalam pengumpulan data penelitian yaitu masyarakat atau kalangan pengguna *e-wallet* di seluruh wilayah Indonesia dengan jenis *e-wallet* apapun. *E-wallet* diambil dikarenakan menjadi sebuah tren di jaman sekarang ini yang melakukan segala jenis transaksi secara non tunai atau *cashless*.

3.2.4 Sampel

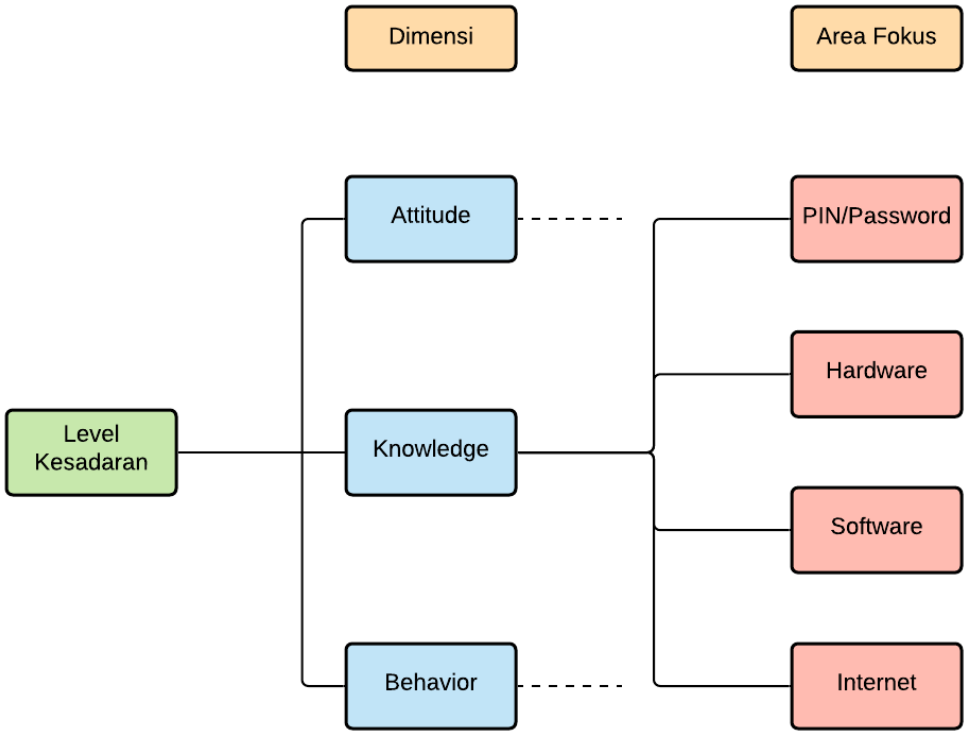
Sampel adalah sebagian dari jumlah dan karakteristik yang dimiliki oleh populasi tersebut, ataupun bagian kecil dari anggota populasi yang diambil menurut prosedur tertentu sehingga dapat mewakili populasinya (Siyoto & Sodik, 2015). Sampel digunakan jika populasi yang di teliti besar, dan peneliti tidak mungkin mempelajari seluruh populasi (Siyoto & Sodik, 2015). Sampel yang akan digunakan dari populasi haruslah benar-benar dapat mewakili populasi yang diteliti (Siyoto & Sodik, 2015).

Sampel yang digunakan dalam pengumpulan data penelitian ini yaitu masyarakat atau kalangan pengguna E-Wallet yang mengisi kuesioner via Google Forms yang disebarkan di beberapa platform sosial media seperti WhatsApp, Telegram, Instagram, Twitter, dan Facebook yang berhasil mengumpulkan 398 orang yang kemudian berkurang menjadi 370 orang setelah dilakukan pembersihan data.

3.3 Instrumen Penelitian

Dalam penelitian ini, instrumen yang digunakan adalah melalui kuesioner yang dijawab oleh responden berupa Google Forms yang telah disebar. Dalam kuesioner tersebut terdapat pertanyaan yang telah disusun sedemikian rupa yang akan dijawab oleh responden sesuai dengan apa yang mereka ketahui atau lakukan. Pertanyaan tersebut dibuat berdasarkan Model Kruger dan Kearney dengan variabel yang diteliti yaitu *knowledge*, *attitude*, dan *behavior*.

Pengukuran kesadaran keamanan yang dikembangkan dengan mengikuti Model Kruger dan Kearney berlandaskan teori psikologi sosial yang membagi tiga komponen untuk mengukur objek yaitu *cognition, affection,* dan *behavior* (Kruger & Kearney, 2006).

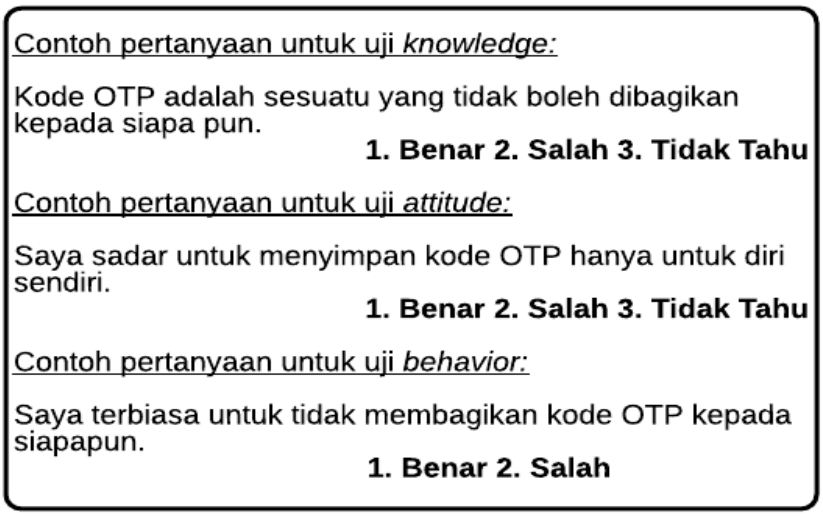


Gambar 3.3 Kerangka Pengukuran Kesadaran Keamanan Informasi

Gambar 3.3 di atas, merupakan kerangka untuk melakukan pengukuran kesadaran keamanan pada kalangan pengguna *e-wallet* di Indonesia berdasarkan Model Kruger dan Kearney dengan variabel yang diteliti yaitu *knowledge, attitude*, dan *behavior*. Pada setiap dimensi akan terdapat empat area fokus yang sama yaitu PIN/Password, *hardware*, *software*, dan Internet. Ada beberapa point penting yang harus diingat ketika menggunakan *e-wallet* yaitu jangan bagikan sandi akun, hindari unduhan yang dilakukan di luar Play Store, jangan hubungkan perangkat ke website yang mencurigakan, jangan kehilangan perangkat, pasang antivirus pada perangkat, jangan simpan detail kartu kredit pada perangkat, tetap jaga kebersihan penyimpanan, dan bijaklah ketika membuka sebuah alamat yang bisa saja mengarah pada *malware* (Kanimozhi. G, 2017). Dari poin penting tersebut dan hasil perumusan pertanyaan yang dibuat untuk kuesioner yang dikelompokkan bersama dosen pembimbing didapatkan ke empat area fokus tersebut.

Area fokus PIN/Password berisikan pertanyaan terkait kata sandi sebagai tindakan pencegahan agar aplikasi *e-wallet* tidak bisa digunakan selain kita yang mengetahui kata sandi tersebut seperti jenis sandi, *lockscreen,* OTP, dan lain sebagainya. Lalu, area fokus *hardware* berisikan pertanyaan terkait perangkat fisik seperti *smartphone* yang kita gunakan untuk keperluan sehari-hari. Pada area fokus ini, bukan merujuk pada komponen fisik di dalam *smartphone* melainkan kepada perlakuan pengguna terhadap *smartphone* seperti diletakkan di tempat yang aman atau tidak ditinggalkan *smartphone* tersebut tanpa pengawasan. Kemudian, area fokus *software* berisikan pertanyaan terkait perangkat lunak yang digunakan pada *smartphone* seperti versi terbaru sistem operasi ataupun versi terbaru dari *e-wallet* yang digunakan ketika melakukan transaksi. Terakhir, area fokus internet berisisikan pertanyaan terkait jaringan internet yang digunakan seperti data seluler ataupun Wi-Fi publik ketika menggunakan aplikasi *e-wallet* tersebut.

Melalui penyesuaian diksi kalimat untuk setiap area fokus pada masing-masing dimensi maka dihasilkan pertanyaan untuk mengukur kesadaran keamanan pengguna *e-wallet* di Indonesia dengan contoh pertanyaan seperti pada Gambar 3.4 di bawah.



Gambar 3.4 Contoh Pertanyaan Kuesioner

Berdasarkan Model Kruger dan Kearney, dibuatlah contoh pertanyaan untuk penelitian ini yang disesuaikan dengan model tersebut dan topik dari penelitian ini yaitu *e-wallet*. Pada dimensi *knowledge* dan *attitude,* diberikan tiga buah opsi jawaban yaitu benar, salah, dan tidak tahu. Sedangkan pada dimensi *behavior* hanya memiliki dua opsi jawaban saja yaitu benar dan salah. Ini dikarenakan pada dimensi *behavior* berkaitan dengan kebiasaan pengguna sehari-hari

yang jika dipikirkan setiap pengguna seharusnya tahu dengan apa saja kebiasaan yang sering mereka lakukan ketika menggunakan *e-wallet* baik itu ketika mengecek saldo, melakukan pembayaran *e-commerce*, penetapan PIN atau *password* yang digunakan, dan lain sebagainya.

3.4 Analisis Data

Dalam penelitian ini, terdapat beberapa pertanyaan terkait demografi seperti jenis kelamin, usia, lokasi yang meliputi pulau, provinsi, dan kabupaten/kota, pendidikan terakhir, dan penghasilan bulanan. Selanjutnya, terdapat total 39 pertanyaan untuk mengukur kesadaran keamanan yang dikembangkan dengan mengikuti model Kruger dan Kearney berlandaskan teori psikologi sosial yang membagi tiga komponen untuk mengukur objek yaitu *cognition, affection,* dan *behavior* (Kruger & Kearney, 2006). Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *Knowledge* (pengetahuan seseorang), *Attitude* (sikap seseorang) dan *Behavior* (perilaku seseorang). Keseluruhan 39 pertanyaan yang digunakan untuk mengukur tingkat kesadaran keamanan dapat dilihat pada Tabel 3.1 di bawah ini.

Tabel 3.1 Daftar Pertanyaan

Dimensi	Pertanyaan	Opsi
Knowledge	1. Penggunaan lockscreen di smartphone, baik itu password, pin, pola, atau biometrik adalah suatu keharusan. 2. Penggunaan password atau pin yang sama untuk beberapa akun berbeda adalah sesuatu yang perlu dihindari. 3. Penggunaan aplikasi e-wallet saat terhubung ke jaringan Wi-Fi publik sebaiknya dihindari. 4. Password/PIN e-wallet tidak boleh dibagikan kepada orang lain. 5. Letakkan dan simpan smartphone hanya di tempat yang aman. 6. Menyimpan password/PIN dalam bentuk catatan berupa teks adalah sesuatu yang perlu dihindari. 7. Kode OTP adalah sesuatu yang tidak boleh dibagikan kepada siapa pun. 8. Instalasi aplikasi dari luar Google Play Store (Android) atau Apple App Store (iOS) adalah sesuatu yang perlu dihindari. 9. Melakukan update sistem operasi di smartphone secara berkala adalah sesuatu yang sebaiknya dilakukan. 10. Membiarkan orang lain menggunakan smartphone tanpa pengawasan si pemilik adalah sesuatu yang harus dihindari. 11. Meninggalkan smartphone tanpa pengawasan langsung adalah sesuatu yang sebaiknya dihindari. 12. Memastikan aplikasi e-wallet menggunakan versi terbaru adalah sesuatu yang sebaiknya dilakukan. 13. Penggunaan password/PIN yang mudah ditebak seperti nama sendiri, tanggal lahir, angka berurutan, atau angka berulang adalah sesuatu yang perlu dihindari.	• Benar • Salah • Tidak Tahu

Attitude	1. Saya sadar untuk menggunakan lockscreen di smartphone, baik itu password, pin, pola, atau biometrik agar lebih aman. 2. Saya sadar untuk menggunakan password atau pin yang berbeda untuk beberapa akun yang digunakan. 3. Saya sadar untuk menggunakan e-wallet hanya melalui data seluler dari sim card sendiri. 4. Saya sadar untuk menyimpan password/PIN e-wallet hanya untuk diri sendiri. 5. Saya sadar untuk meletakkan dan menyimpan smartphone hanya di tempat yang aman. 6. Saya sadar untuk menghindari password/PIN e-wallet yang disimpan dalam bentuk catatan berupa teks. 7. Saya sadar untuk menyimpan kode OTP hanya untuk diri sendiri. 8. Saya sadar untuk menginstall aplikasi hanya dari Google Play Store (Android) atau Apple App Store (iOS). 9. Saya sadar untuk melakukan update sistem operasi di smartphone secara berkala. 10. Saya sadar untuk mengawasi smartphone milik sendiri ketika sedang digunakan oleh orang lain. 11. Saya sadar untuk meninggalkan smartphone di tempat yang bisa diawasi langsung oleh diri sendiri. 12. Saya sadar untuk memastikan aplikasi e-wallet menggunakan versi terbaru ketika hendak melakukan transaksi/pembayaran. 13. Saya sadar untuk menggunakan password /PIN yang kompleks agar tidak mudah ditebak.	• Benar • Salah • Tidak Tahu
Behavior	1. Saya terbiasa melakukan pengamanan menggunakan lockscreen di smartphone, baik itu password, pin, pola, atau biometrik. 2. Saya terbiasa untuk tidak menggunakan password atau pin yang sama untuk beberapa akun berbeda. 3. Saya terbiasa untuk tidak menggunakan e-wallet ketika terhubung ke jaringan Wi-Fi publik. 4. Saya terbiasa untuk tidak membagikan password/PIN e-wallet kepada orang lain. 5. Saya terbiasa untuk tidak meletakkan dan menyimpan smartphone di tempat sembarangan. 6. Saya terbiasa untuk tidak menyimpan password/PIN dalam bentuk catatan berupa teks. 7. Saya terbiasa untuk tidak membagikan kode OTP kepada siapapun. 8. Saya terbiasa melakukan penginstalan aplikasi hanya dari Google Play Store (Android) atau Apple App Store (iOS). 9. Saya terbiasa melakukan update sistem operasi di smartphone secara berkala. 10. Saya terbiasa untuk tidak membiarkan orang lain menggunakan smartphone milik saya tanpa pengawasan. 11. Saya terbiasa untuk tidak meninggalkan smartphone tanpa pengawasan langsung 12. Saya terbiasa melakukan pengecekan versi terbaru aplikasi e-wallet yang hendak digunakan. 13. Saya terbiasa untuk tidak menggunakan password/PIN yang mudah ditebak seperti nama sendiri, tanggal lahir, angka berurutan, atau angka berulang.	• Benar • Salah

Data yang telah dikumpulkan untuk penelitian ini akan dianalisis secara kuantitatif. Pertama, dilakukan perhitungan skor kesadaran keamanan untuk masing-masing responden

berdasarkan jawaban dari instrumen yang digunakan untuk mengukur tingkat kesadaran keamanan. Untuk pilihan pada pertanyaan yang dijawab benar oleh responden akan mendapat nilai 10. Lalu untuk pilihan pada pertanyaan yang dijawab tidak tahu oleh responden akan mendapat nilai 5. Kemudian, untuk pilihan pada pertanyaan yang dijawab salah maka akan diberikan nilai 0. Penilaian berdasarkan skala ordinal yang merupakan skala pengukuran yang menyatakan peringkat antar tingkatan di mana jarak atau interval antar tingkatan juga tidak harus sama (Janna, 2020). Nilai responden untuk setiap soal akan ditentukan melalui kriteria penilaian yang telah dijelaskan berdasarkan pilihan jawaban yang mereka pilih dengan jujur sesuai apa yang mereka rasakan atau alami selama ini sesuai dengan keseharian yang dilakukan.

Kemudian, perlu dilakukan pembobotan pada dimensi dan area fokus. Pembobotan kesadaran ditentukan menggunakan *Analytical Hierarchy Process* (AHP) (Kencana Sari & Candiwan, 2014). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi subyektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen (Akraman et al., 2018). Setiap dimensi akan memiliki bobot masing-masing yang digunakan dalam perhitungan kesadaran atau *awareness* nantinya. Berikut pembagian bobot untuk dimensi dan pertanyaan untuk area fokus yang dapat dilihat pada Tabel 3.2 dan Tabel 3.3.

Tabel 3.2 Pembagian Bobot Dimensi

Dimensi	**Bobot**
Knowledge	30%
Attitude	20%
Behavior	50%

Sumber: Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296.

Tabel 3.3 Pembagian Pertanyaan untuk Tiap Area Fokus

Area Fokus	**Pertanyaan**
PIN/Password	1,2,4,6,7,13
Hardware	5,10,11
Software	1,8,9,12
Internet	3,7,8

Dari data yang telah dikumpulkan melalui Google Forms didapatkan 398 responden yang mengisi kuesioner tersebut. Tetapi sebelum dilanjutkan untuk proses analisis, harus dilakukan terlebih dahulu pembersihan data. Pembersihan data bertujuan untuk menghapus data yang terindikasi sebuah duplikasi atau data yang sama persis terdapat dua kali atau lebih pengisiannya. Selain itu, pembersihan data pun bertujuan untuk menghapus data yang tidak sesuai dengan kriteria responden yang dibutuhkan dalam penelitian. Setelah dilakukan proses pembersihan data, maka didapatkan 370 data yang bersih dari duplikasi ataupun yang tidak sesuai dengan kriteria responden yang dibutuhkan dalam penelitian ini.

Setelah pembersihan data, maka dilakukan perhitungan tingkat kesadaran keamanan dari data yang telah dikumpulkan sebelumnya. Perhitungan dibagi menjadi 5 tahap yaitu penjumlahan nilai pertanyaan yang dijawab responden untuk masing-masing area fokus pada setiap dimensi, perhitungan nilai kesadaran untuk masing-masing area fokus pada setiap dimensi, perhitungan nilai total kesadaran fokus area, perhitungan nilai total kesadaran dimensi dan perhitungan nilai kesadaran secara keseluruhan. Tahap pertama yaitu penjumlahan nilai pertanyaan yang dijawab responden untuk masing-masing area fokus pada setiap dimensi melalui persamaan (3.1).

$$JNJ = NJ_1 + NJ_2 + NJ_3 + \cdots + NJ_n \qquad (3.1)$$

Keterangan:

JNJ: jumlah nilai jawaban responden

NJ: nilai jawaban responden

n: pembagian pertanyaan untuk tiap area fokus

Lalu, tahap kedua yaitu perhitungan nilai kesadaran untuk masing-masing area fokus pada setiap dimensi melalui persamaan (3.2) dan (3.3). Perhitungan dilakukan pada setiap dimensi untuk memudahkan analisis data agar tidak terlalu banyak atau tertumpuk pada *sheets* yang sama.

$$TJNJ = \left(\frac{JNJ_1}{JBP_i}/10\right) + \left(\frac{JNJ_2}{JBP_i}/10\right) + \left(\frac{JNJ_3}{JBP_i}/10\right) + \cdots + \left(\frac{JNJ_n}{JBP_i}/10\right) \qquad (3.2)$$

$$NKAF = \frac{TJNJ}{JR} \text{x} 100 \quad (3.3)$$

Keterangan:

TJNJ: jumlah nilai jawaban dari seluruh responden

NKAF: nilai kesadaran area fokus pada masing-masing dimensi

JNJ_n: jumlah nilai jawaban responden ke-n

JBP_i: jumlah bobot pertanyaan area fokus ke-i

JR: jumlah responden

Selanjutnya, tahap ketiga yaitu perhitungan nilai total kesadaran untuk masing-masing fokus area melalui persamaan (3.4). Nilai total kesadaran berkisar antara 0 – 100 yang berupa dalam persen.

$$TNKAF = (NKAF_1 \text{x} 0{,}3) + (NKAF_2 \text{x} 0{,}2) + (NKAF_3 \text{x} 0{,}5) \quad (3.4)$$

Keterangan:

TNKAF: total nilai kesadaran untuk masing-masing area fokus

$NKAF_1$: nilai kesadaran area fokus pada dimensi 1 (*Knowledge*)

$NKAF_2$: nilai kesadaran area fokus pada dimensi 2 (*Attitude*)

$NKAF_3$: nilai kesadaran area fokus pada dimensi 3 (*Behavior*)

Kemudian, tahap keempat yaitu perhitungan nilai total kesadaran untuk masing-masing dimensi melalui persamaan (3.5). Nilai total kesadaran berkisar antara 0 – 100 yang berupa dalam persen.

$$TNKD = (NKD_1 + NKD_2 + NKD_3 + NKD_4)/4 \quad (3.5)$$

Keterangan:

TNKD: total nilai kesadaran untuk masing-masing dimensi

NKD_1: nilai kesadaran area fokus 1 (PIN/Password)

NKD_2: nilai kesadaran area fokus 2 (*Hardware*)

NKD_3: nilai kesadaran area fokus 3 (*Software*)

NKD_4: nilai kesadaran area fokus 4 (Internet)

Terakhir, tahap kelima yaitu perhitungan nilai kesadaran secara keseluruhan sebagai hasil akhir nilai kesadaran keamanan pengguna E-Wallet di Indonesia melalui persamaan (3.6), (3.7), dan (3.8). Nilai total kesadaran berkisar antara 0 – 100 yang berupa dalam persen.

$$RTNKAF = (TNKAF_1 + TNKAF_2 + TNKAF_3 + TNKAF_4)/4 \quad (3.6)$$

$$RTNKD = (TNKD_1 \text{x} 0{,}3) + (TNKD_2 \text{x} 0{,}2) + (TNKD_3 \text{x} 0{,}5) \quad (3.7)$$

$$NKS = \frac{RTNKAF + RTNKD}{2} \quad (3.8)$$

Keterangan:

NKS: nilai kesadaran keseluruhan

RTNKAF: rata total nilai kesadaran untuk masing-masing area fokus

RTNKD: rata total nilai kesadaran untuk masing-masing dimensi

$TNKAF_1$: total nilai kesadaran area fokus 1 (PIN/Password)

$TNKAF_2$: total nilai kesadaran area fokus 2 (*Hardware*)

$TNKAF_3$: total nilai kesadaran area fokus 3 (*Software*)

$TNKAF_4$: total nilai kesadaran area fokus 4 (Internet)

$TNKD_1$: total nilai kesadaran area fokus pada dimensi 1 (*Knowledge*)

$TNKD_2$: total nilai kesadaran area fokus pada dimensi 2 (*Attitude*)

$TNKD_3$: total nilai kesadaran area fokus pada dimensi 3 (*Behavior*)

Dari hasil perhitungan tingkat kesadaran yang didapatkan, maka akan didapatkan nilai yang dapat merepresentasikan tingkat kesadaran pengguna *e-wallet*, baik secara keseluruhan responden penelitan, individu, maupun kelompok individu yang akan dievaluasi sesuai kriteria yang tertera pada Tabel 3.4 yang merupakan hasil penyesuaian dari model Kruger dan Kearney khusus untuk penelitian ini. Kriteria kesadaran berikut, yang didefinisikan sesuai dengan pandangan manajemen tentang kinerja kesadaran yang digunakan untuk menjelaskan tingkat kesadaran (Kruger & Kearney, 2006).

Tabel 3.4 Kriteria Kesadaran

Kriteria	Nilai (%)	Keterangan
Baik	95 – 100	Sudah baik, perlu dipertahankan
Rata-Rata	80 – 94	Cukup baik, namun masih terbuka peluang ditingkatkan
Buruk	Kurang dari 80	Perlu perhatian khusus untuk upaya peningkatan

Sumber: Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296.

Selanjutnya, untuk mengukur perbedaan tingkat kesadaran keamanan antar kelompok demografi yang berbeda sekaligus menginvestigasi pengaruh perbedaan faktor demografis tersebut, akan dilakukan analisis lanjutan berupa regresi linear berganda *(multiple linear regression)* dengan metode OLS *(ordinary least squares)* dengan nilai atau skor kesadaran keamanan sebagai *dependent variable* dan berbagai faktor demografi responden sebagai *independent variables*.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Karakteristik Responden

Tabel 4.1 di bawah berisikan informasi karakteristik 370 orang responden dalam penelitian ini setelah melalui proses pembersihan data. Informasi tersebut disajikan dalam berbagai kategori sesuai informasi demografi yang meliputi jenis kelamin, usia, lokasi, pendidikan, dan penghasilan.

Tabel 4.1 Karakteristik Responden

Karakteristik	Jumlah	Persen
Jenis Kelamin		
Laki-Laki	188	50,81%
Perempuan	182	49,19%
Usia		
< 25 Tahun	232	62,70%
25 – 34 Tahun	82	22,16%
≥ 35 Tahun	56	15,14%
Lokasi		
Kota	134	36,22%
Kabupaten	236	63,78%
Asal Daerah		
Pulau Jawa	307	82,97%
Non-Jawa	63	17,03%
Pendidikan Terakhir		
Dasar-Menengah	228	61,62%
Perguruan Tinggi	142	38,38%
Penghasilan Bulanan		
< Rp1 juta	165	44,59%
Rp1-2.99 juta	102	27,57%
Rp3-4.99 juta	42	11,35%
≥ Rp5 juta	61	16,49%

Karakteristik responden didapatkan dari hasil kuesioner yang sudah disebarkan diberbagai platform sosial media dengan enam variabel demografi diantaranya jenis kelamin, usia, lokasi berdasarkan kabupaten/kota, asal daerah berdasarkan pulau jawa dan non-jawa,

pendidikan terakhir, dan penghasilan bulanan. Dari segi jenis kelamin, kuesioner ini diisi oleh kedua jenis kelamin laki-laki dan perempuan secara cukup berimbang dengan persentase secara berurut yaitu 50,81% dan 49,19%.

Dari segi usia, kuesioner ini didominasi oleh responden dengan usia di bawah 25 tahun yang mencapai 62,70% dari total responden. Usia 25 sampai 34 tahun hanya mencapai 22,16% dan usia 35 tahun dan di atasnya hanya mencapai 15,14%. Hal ini bisa disebabkan karena mayoritas usia di bawah 25 tahun adalah pelajar atau mahasiswa yang sedang menempuh pendidikan pada tahun 2020 yang biasanya identik dengan sebutan kaum *millennial*. Kaum *millennial* ini erat kaitannya dengan cepatnya beradaptasi dengan teknologi yang bermunculan, sama halnya dengan teknologi *e-wallet* sebagai alat pembayaran non-tunai. Generasi *millennial* adalah generasi yang sangat mahir dalam menggunakan teknologi yang menyebabkan generasi ini memiliki banyak peluang untuk jauh berada di depan dibandingkan generasi sebelumnya (Khadijah, 2019).

Selanjutnya dari segi lokasi, mayoritas responden berasal dari daerah kabupaten yang mencapai 63,78% persen dibandingkan dengan responden yang berasal dari kota. Responden yang berasal dari daerah kota hanya mencapai 36,22% dari total responden. Ini disebabkan oleh lebih banyaknya jumlah kabupaten dibandingkan kota yang ada di Indonesia. Menurut Badan Pusat Statistik (BPS), jumlah kabupaten di Indonesia adalah 416 kabupaten, sedangkan jumlah kota di Indonesia adalah 98 kota (Badan Pusat Statistik, 2019).

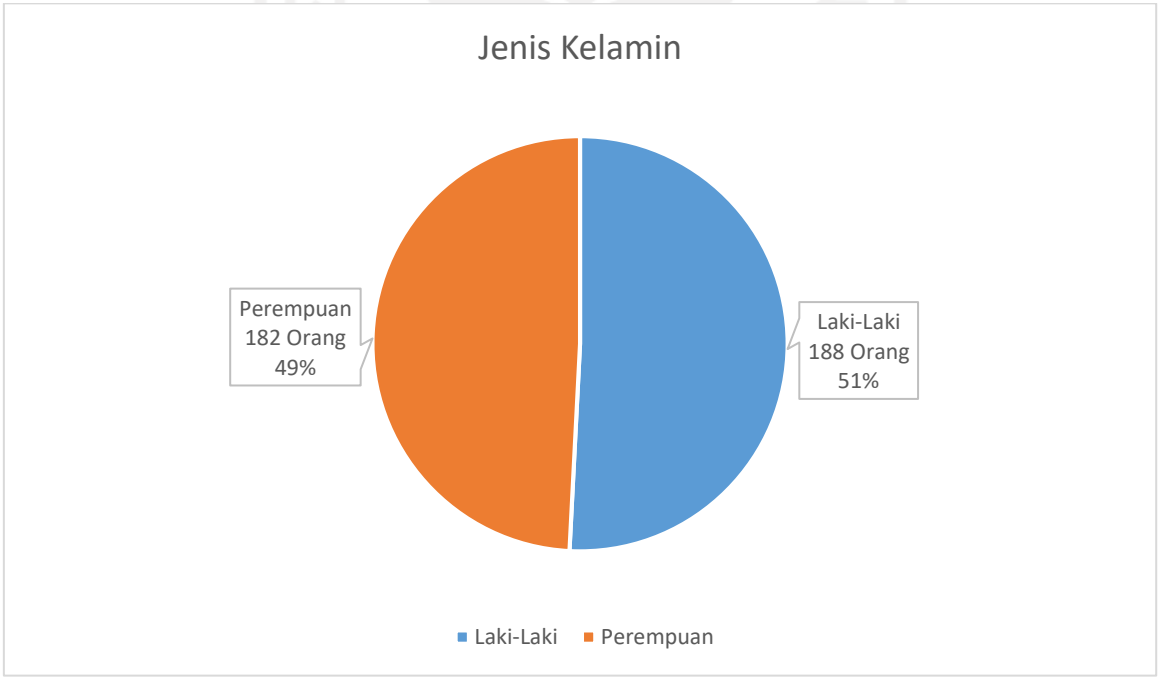
Dari segi asal daerah, mayoritas responden berasal dari Pulau Jawa dengan jumlah 307 orang dengan persentase 82,97%. Sedangkan 63 orang lainnya berasal dari berbagai macam pulau di luar Jawa seperti Sumatera, Kalimantan, Nusa Tenggara, Papua, dan lain sebagainya dengan persentase 17,03%. Ini bisa disebabkan karena kepadatan penduduk yang dimiliki Pulau Jawa tertinggi dibandingkan dengan pulau lainnya. Menurut Badan Pusat Statistik (BPS), penduduk di Pulau Jawa pada tahun 2019 mencapai 150,4 juta jiwa yang jumlah tersebut setara dengan separuh penduduk di Indonesia yang mencapai 266,91 juta jiwa (Badan Pusat Statistik, 2019). Alasan lainnya yang mempengaruhi seperti aktivitas bisnis yang memang didominasi daerah Jabodetabek di Pulau Jawa yang menyebabkan pengguna *e-wallet* yang lebih banyak dan sering memakainya untuk berbagai keperluan. Menurut Direktur Neraca Pengeluaran Badan Pusat Statistik (BPS) Pudji Agus Kurniawan mengatakan, tren jual beli barang melalui digital atau *online* sebagian besar masih didominasi oleh masyarakat di Jawa dikarenakan memiliki infrastruktur dan sistem produksi yang bagus dibanding wilayah lain (Situmorang, n.d.).

Dari segi pendidikan terakhir, sebesar 61,62% didominasi oleh responden yang dengan pendidikan terakhir di jenjang pendidikan dasar atau menengah dibandingkan yang sudah menamatkan studi di perguruan tinggi. Untuk responden yang memiliki pendidikan terakhir di perguruan tinggi baik D3, S1, S2, dan S3 hanya sebesar 38,38%. Ini berkaitan dengan usia sebelumnya yang mayoritas usia di bawah 25 tahun merupakan pelajar atau mahasiswa yang sedang menempuh pendidikan tinggi.

Dari segi penghasilan bulanan, hampir separuh responden memiliki penghasilan bulanan kurang dari Rp.1.000.000 yang dikarenakan tingginya angka pelajar dan mahasiswa yang menjadi responden dalam penelitian ini dengan persentase sebesar 44,59%. Penghasilan bulanan lainnya yaitu Rp.1.000.000 – Rp.2.999.999, Rp.3.000.000 – Rp.4.999.999, dan Rp.5.000.000 ke atas secara berurutan memiliki persentase sebesar 27,57%, 11,35%, dan 16,49%.

4.1.1 Jenis Kelamin Responden

Berikut persentase jenis kelamin responden dalam bentuk grafik dapat dilihat pada Gambar 4.1.



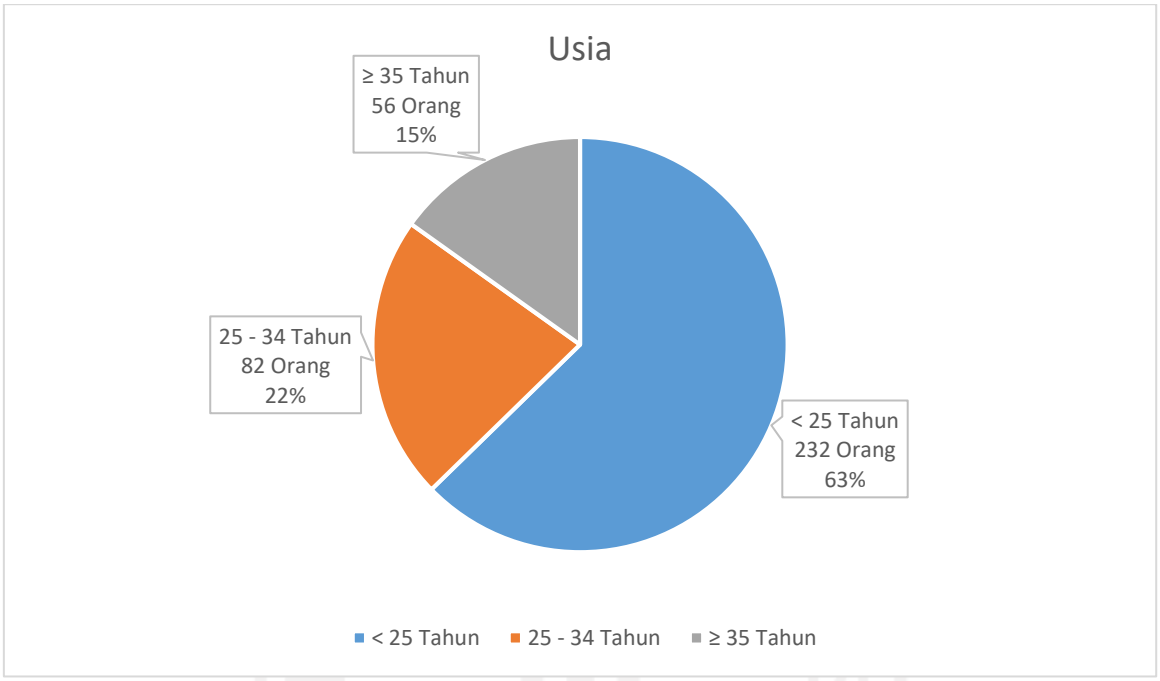
Gambar 4.1 Responden Menurut Jenis Kelamin

Berdasarkan Gambar 4.1 menunjukkan bahwa responden dari penelitian ini memliki perbandingan yang hampir seimbang antara laki-laki dan perempuan. Responden laki-laki

berjumlah 188 orang dengan persentase 51%, sedangkan responden perempuan berjumlah 182 orang dengan persentase 49%.

4.1.2 Usia Responden

Berikut persentase usia responden dengan kategorinya dalam bentuk grafik dapat dilihat pada Gambar 4.2.

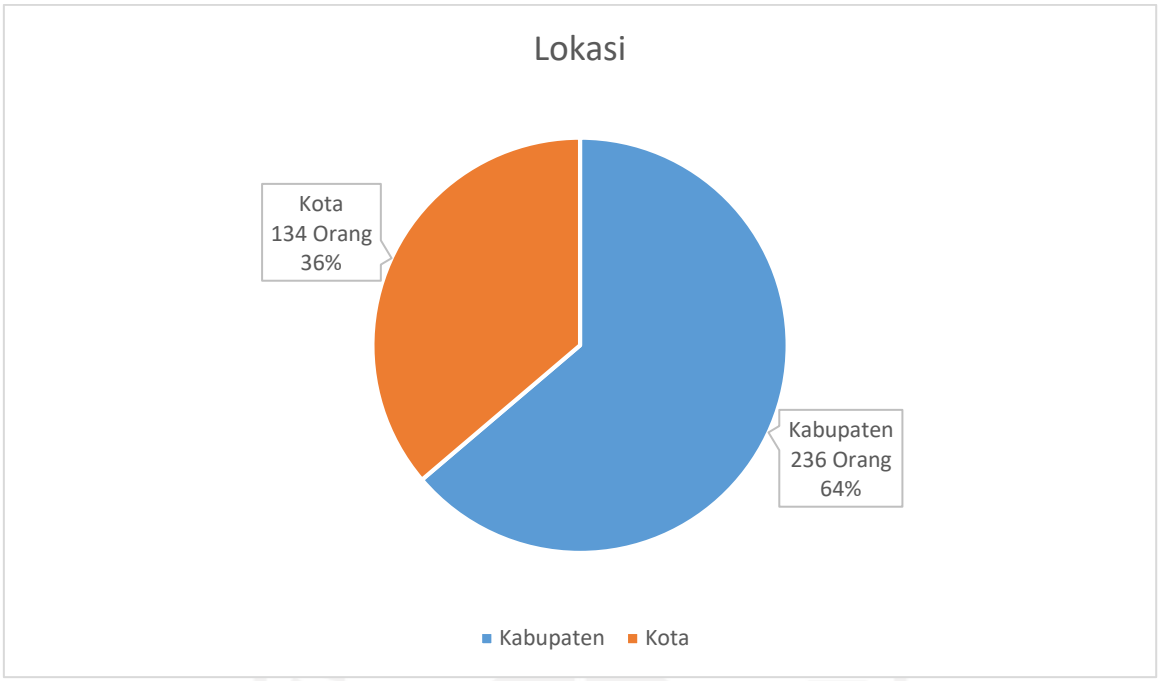


Gambar 4.2 Responden Menurut Usia

Berdasarkan Gambar 4.2 menunjukkan bahwa mayoritas responden dari penelitian ini adalah pengguna yang berusia di bawah 25 tahun berjumlah 232 orang dengan persentase 63%. Lalu, untuk 37% sisanya terbagi menjadi 2 kelompok yaitu pengguna yang berusia 25 – 34 tahun berjumlah 82 orang dengan persentase 22% dan pengguna yang berusia 35 ke atas berjumlah 56 orang dengan persentase 15%.

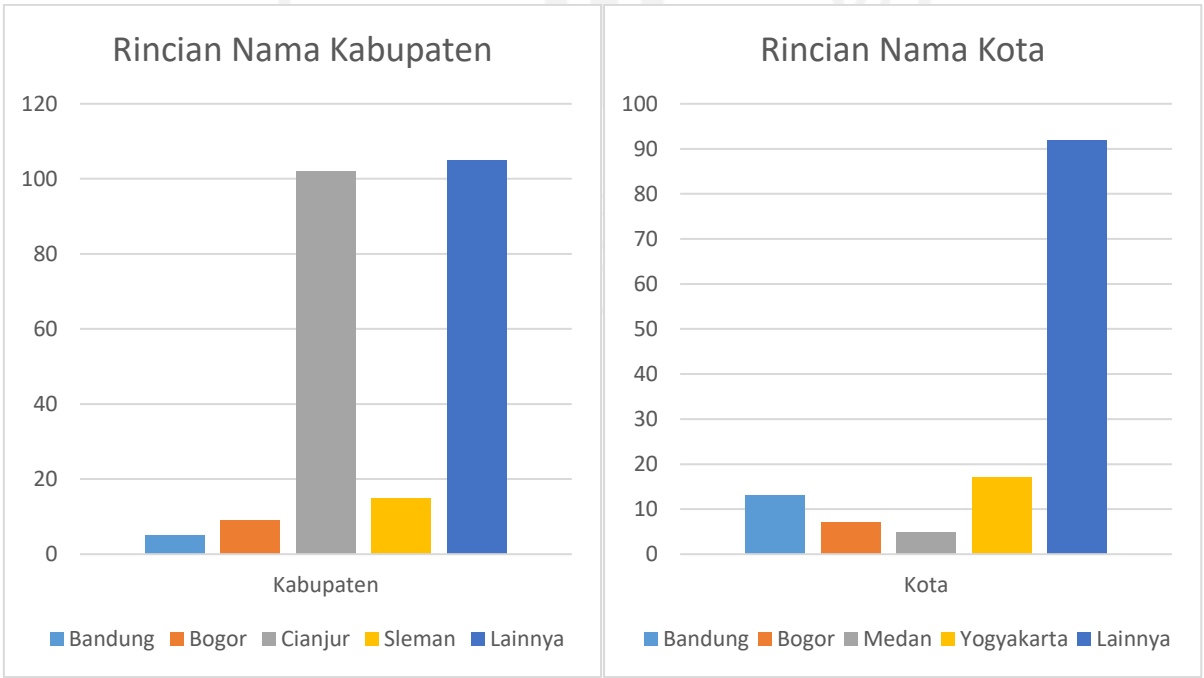
4.1.3 Lokasi Responden

Berikut persentase lokasi responden berdasarkan asal kabupaten/kota dalam bentuk grafik dapat dilihat pada Gambar 4.3.



Gambar 4.3 Responden Menurut Lokasi

Berdasarkan Gambar 4.3 menunjukkan bahwa mayoritas responden dari penelitian ini adalah pengguna yang berasal dari kabupaten berjumlah 236 orang dengan persentase 64%. Kemudian, pengguna yang berasal dari kota berjumlah 134 orang dengan persentase 36%. Untuk rincian nama kabupaten/kota dapat dilihat pada grafik di bawah.



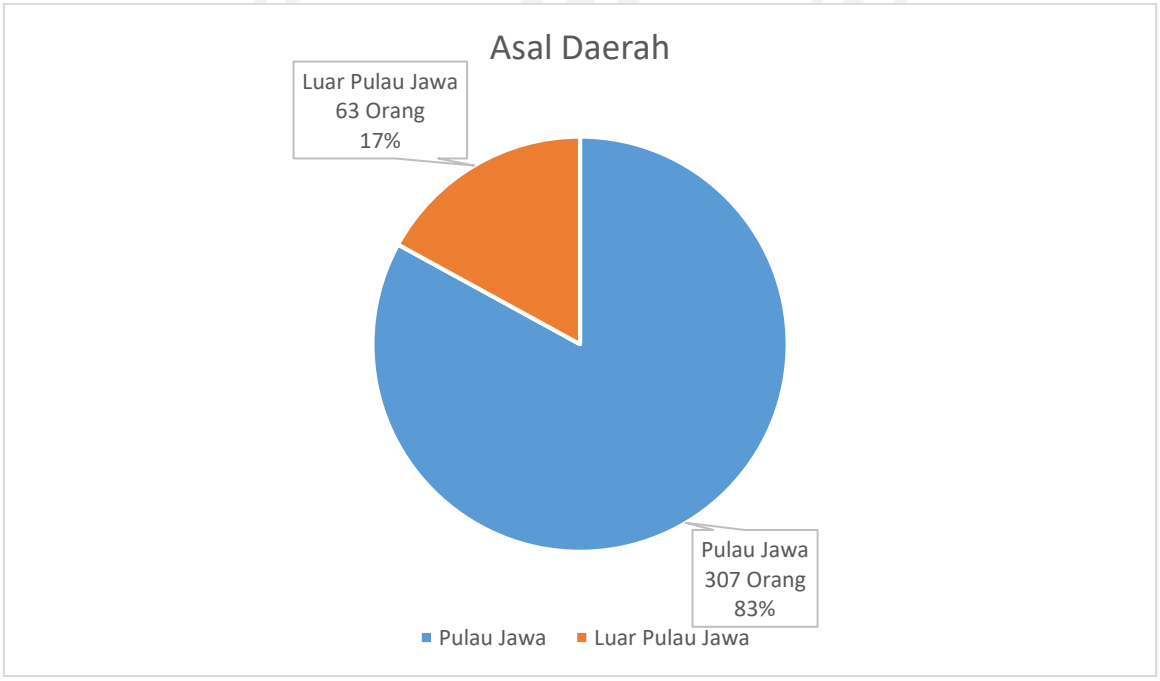
Gambar 4.4 Rincian Nama Kabupaten dan Kota

Berdasarkan Gambar 4.4 menunjukkan bahwa Kabupaten Cianjur merupakan responden terbanyak yang berasal dari lokasi kabupaten dengan jumlah sebanyak 102 orang. Disusul oleh Kabupaten Sleman, Kabupaten Bogor, dan Kabupaten Bandung secara berurutan dengan jumlah sebanyak 15 orang, 9 orang, dan 5 orang. Selain dari yang disebutkan pada grafik dicampur pada kabupaten lainnya yang berjumlah 105 orang meliputi Kabupaten Ciamis, Kabupaten Purwakarta, Kabupaten Bekasi, Kabupaten Kotawaringin Barat, Kabupaten Jayapura, dan lain sebagainya yang ada di Indonesia.

Kemudian, berdasarkan Gambar 4.4 pun menunjukkan bahwa Kota Yogyakarta menjadi penyumbang responden terbanyak yang berasal dari lokasi kota dengan jumlah sebanyak 17 orang. Disusul oleh Kota Bandung, Kota Bogor, dan Kota Medan secara berurutan dengan jumlah sebanyak 13 orang, 7 orang, dan 5 orang. Selain dari yang disebutkan pada grafik dicampur pada kota lainnya yang berjumlah 92 orang meliputi Kota Tangerang Selatan, Kota Jakarta Pusat, Kota Pekanbaru, Kota Banjarmasin, Kota Batam, dan lain sebagainya yang ada di Indonesia.

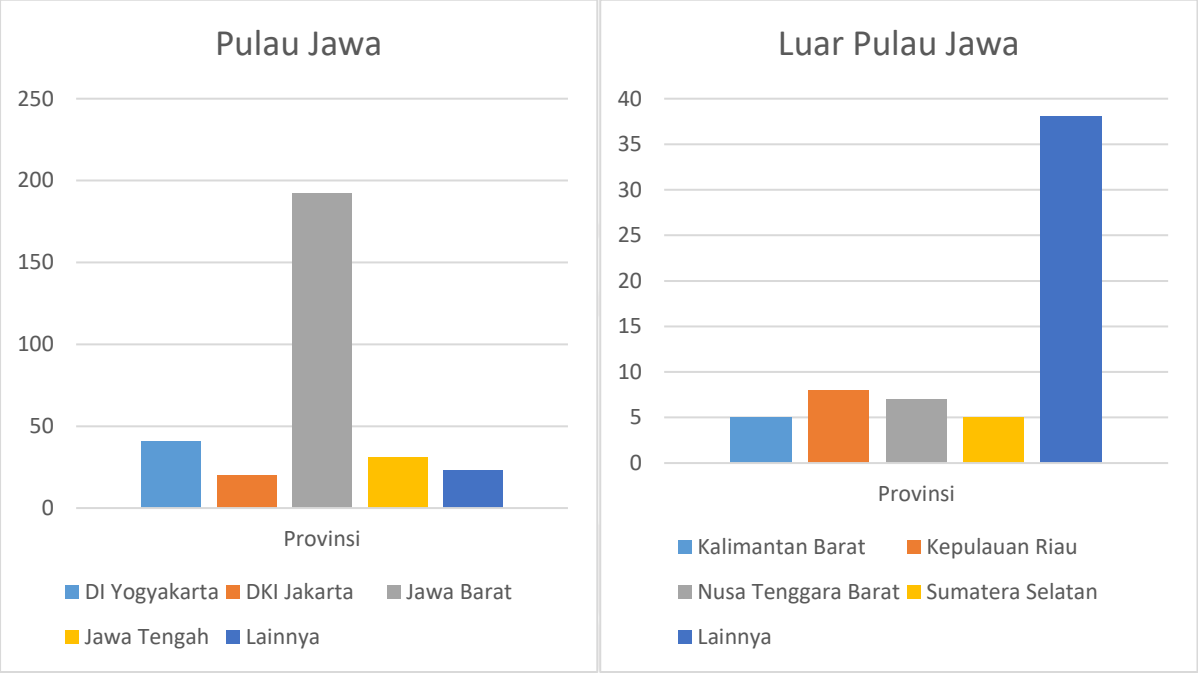
4.1.4 Asal Daerah Responden

Berikut persentase asal daerah responden yang berasal dari Pulau Jawa dan luar Pulau Jawa dalam bentuk grafik dapat dilihat pada Gambar 4.5.



Gambar 4.5 Responden Menurut Asal Daerah

Berdasarkan Gambar 4.5 menunjukkan bahwa mayoritas responden dari penelitian ini adalah pengguna yang berasal dari Pulau Jawa berjumlah 307 orang dengan persentase 83%. Kemudian, pengguna yang berasal dari luar Pulau Jawa berjumlah 63 orang dengan persentase 17%. Untuk rincian nama provinsi dari asal daerah dapat dilihat pada grafik di bawah.



Gambar 4.6 Rincian Provinsi Asal Daerah

Berdasarkan Gambar 4.6 menunjukkan bahwa Provinsi Jawa Barat merupakan responden terbanyak dari Pulau Jawa dengan jumlah sebanyak 192 orang. Disusul oleh Provinsi DI Yogyakarta, Provinsi DKI Jakarta, dan Provinsi Jawa Tengah secara berurutan dengan jumlah sebanyak 41 orang, 20 orang, dan 31 orang. Selain dari yang disebutkan pada grafik dicampur pada provinsi lainnya yang ada di Pulau Jawa berjumlah 23 orang meliputi Provinsi Banten dan Provinsi Jawa Timur.

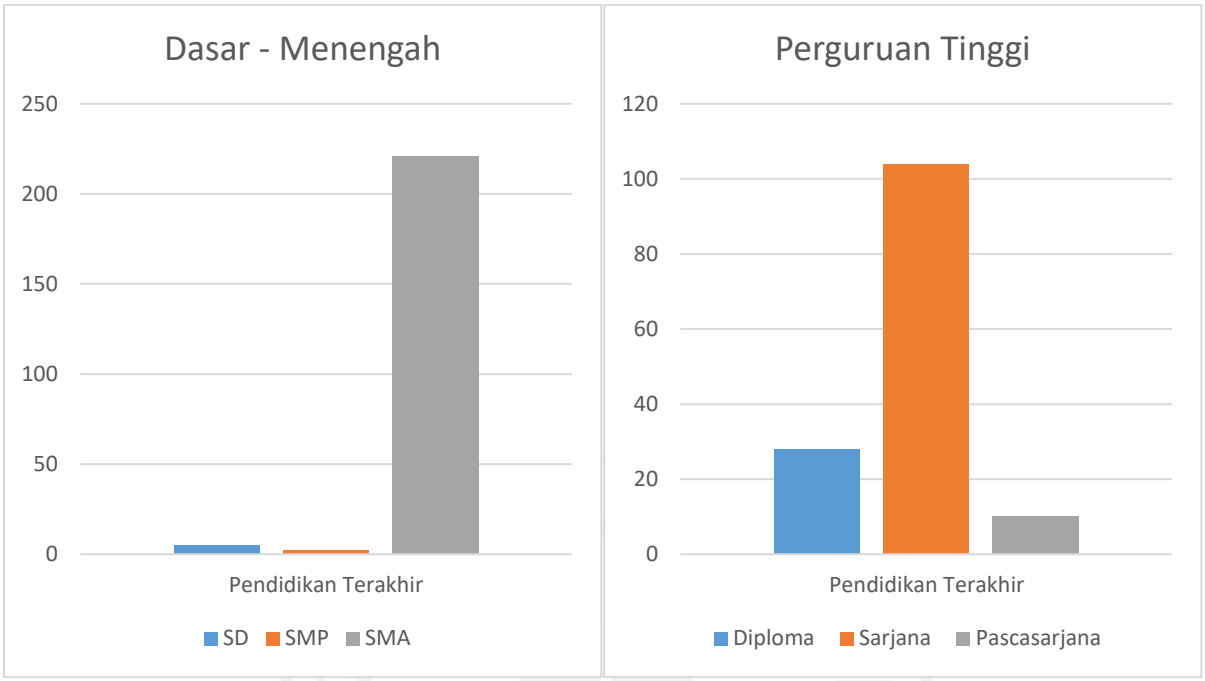
Kemudian, berdasarkan Gambar 4.6 pun menunjukkan bahwa Provinsi Kepualauan Riau merupakan responden terbanyak yang berasal dari luar Pulau Jawa dengan jumlah sebanyak 8 orang. Disusul oleh Provinsi Nusa Tenggara Barat, Provinsi Kalimantan Barat, dan Provinsi Sumatera Selatan secara berurutan dengan jumlah sebanyak 7 orang, 5 orang, dan 5 orang. Selain dari yang disebutkan pada grafik dicampur pada provinsi lainnya yang ada di luar Pulau Jawa berjumlah 38 orang meliputi Provinsi Bali, Provinsi Jambi, Provinsi Lampung, Provinsi Sulawesi Tengah, Provinsi Papua, dan lain sebagainya yang ada di Indonesia.

4.1.5 Pendidikan Terakhir Responden

Berikut persentase pendidikan terakhir responden dalam bentuk grafik dapat dilihat pada Gambar 4.7.

Gambar 4.7 Responden Menurut Pendidikan Terakhir

Berdasarkan Gambar 4.7 menunjukkan bahwa mayoritas pendidikan terakhir responden dari penelitian ini adalah pendidikan dasar sampai menengah berjumlah 228 orang dengan persentase 62%. Lalu, untuk responden yang memiliki pendidikan perguruan tinggi berjumlah 142 orang dengan persentase 38%. Untuk rincian pendidikan terakhir pada masing-masing kategori dapat dilihat pada grafik di bawah.



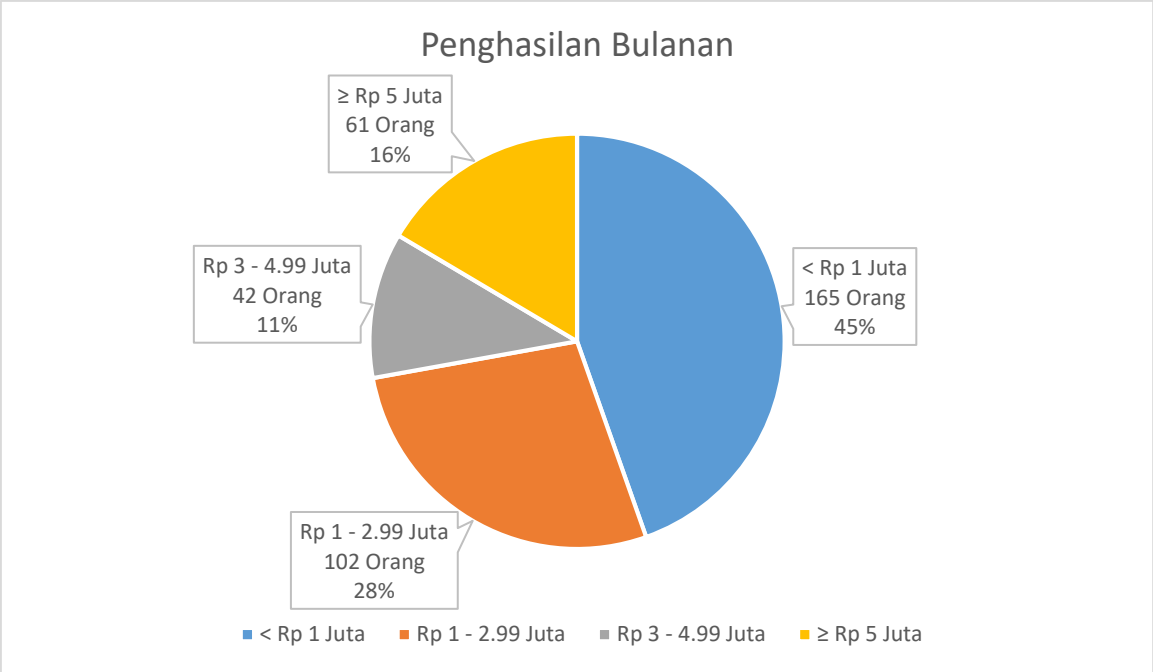
Gambar 4.8 Rincian Pendidikan Terakhir

Berdasarkan Gambar 4.8 menunjukkan bahwa hampir seluruh responden pada kategori dasar sampai menengah merupakan lulusan SMA dengan jumlah sebanyak 221 orang. Hanya sedikit saja responden yang pendidikan terakhirnya lulusan SD berjumlah 5 orang dan lulusan SMP berjumlah 2 orang.

Kemudian, berdasarkan Gambar 4.8 pun menunjukkan bahwa mayoritas responden merupakan lulusan sarjana dengan jumlah sebanyak 104 orang. Disusul oleh lulusan Diploma dan Pascasarjana secara berurutan berjumlah 28 orang dan 10 orang pada penelitian ini.

4.1.6 Penghasilan Bulanan Responden

Berikut persentase penghasilan bulanan responden dalam bentuk grafik dapat dilihat pada Gambar 4.9.



Gambar 4.9 Responden Menurut Penghasilan Bulanan

Berdasarkan Gambar 4.9 menunjukkan bahwa mayoritas responden berpenghasilan di bawah Rp. 1.000.000 setiap bulannya yang berjumlah 165 orang dengan persentase 45%. Selanjutnya, responden dengan penghasilan Rp. 1.000.000 sampai Rp. 2.999.999 per bulannya berjumlah 102 orang dengan persentase 28%. Lalu, responden dengan penghasilan Rp. 3.000.000 sampai Rp. 4.999.999 berjumlah 42 orang dengan persentase 11%. pendidikan terakhir responden dari penelitian ini adalah pendidikan dasar sampai menengah berjumlah 228 orang dengan persentase 62%. Kemudian, untuk responden yang memiliki penghasilan bulanan di atas Rp. 5.000.000 berjumlah 61 orang dengan persentase 16%.

4.2 Hasil Skor Kesadaran Keamanan

Selanjutnya, dilakukan perhitungan skor kesadaran keamanan di kalangan pengguna *e-wallet* di Indonesia yang hasilnya dapat dilihat pada Gambar 4.10 di bawah ini. Skor kesadaran keamanan ini meliputi skor dari masing-masing dimensi dan area fokus yang kemudian menghasilkan skor akhir kesadaran keamanan secara menyeluruh.

Fokus Area / Dimensi (Bobot)	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area
PIN/Password	89	93	89	**90**
Hardware	97	98	95	**96**
Software	89	92	88	**89**
Internet	84	90	88	**87**
Total Kesadaran/Dimensi	**90**	**93**	**90**	**91**

Baik Rata-Rata Buruk

Gambar 4.10 Tingkat Kesadaran Keamanan Informasi Pengguna E-Wallet di Indonesia

Untuk keseluruhan pengguna *e-wallet* di Indonesia, didapatkan skor 91 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge*, *attitude*, maupun *behavior* juga memiliki nilai rata-rata di rentang 90 hingga 93. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 95 hingga 98. Dengan kata lain, kesadaran keamaan terkait isu *hardware* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software*, dan internet walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Sebagai contoh, pertanyaan yang nilainya relatif masih rendah pada area fokus PIN/password yaitu saya terbiasa untuk tidak menggunakan password atau pin yang sama untuk beberapa akun berbeda. Hal ini bisa disebabkan karena banyak orang takut lupa jika password setiap akun yang dimiliki berbeda satu sama lain. Oleh sebab itu, terkait isu PIN/Password hal yang masih perlu ditingkatkan adalah pada penggunaan password yang harusnya berbeda antara satu akun dengan lainnya. Kemudian, pertanyaan yang nilainya relatif

masih rendah pada area fokus *software* yaitu saya terbiasa melakukan pengecekan versi terbaru aplikasi *e-wallet* yang hendak digunakan. Ini disebabkan oleh ketidakbiasaan pengguna untuk mengecek selalu versi terbaru aplikasi dikarenakan merepotkan dan mungkin dianggap hal sepele. Terkait isu *software* hal yang masih perlu ditingkatkan adalah pada pembiasaan pengguna untuk mengecek versi aplikasi *e-wallet* apakah sudah terbaru atau belum. Terakhir, pertanyaan yang nilainya relatif masih rendah pada area fokus internet yaitu saya terbiasa untuk tidak menggunakan *e-wallet* ketika terhubung ke jaringan Wi-Fi publik. Hal ini disebabkan oleh ketidaktahuan pengguna tentang bahayanya menggunakan aplikasi *e-wallet* lewat Wi-Fi publik karena banyak orang umum menggunakannya dan bisa saja melakukan peretasan atau pencurian data melalui jaringan tersebut. Terkait isu internet, hal yang masih perlu ditingkatkan adalah pada pembiasaan pengguna untuk hanya menggunakan data seluler ketika menggunakan *e-wallet* agar aman dari pencurian data lewat jaringan publik.

4.2.1 Skor Kesadaran Keamanan Berdasarkan Jenis Kelamin

	Laki-Laki				Perempuan			
Fokus Area \ **Dimensi (Bobot)**	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area
PIN/Password	89	93	91	**91**	88	93	87	**89**
Hardware	95	97	94	**95**	98	98	96	**97**
Software	90	91	89	**90**	88	93	88	**89**
Internet	83	88	87	**86**	85	92	88	**88**
Total Kesadaran/Dimensi	**89**	**92**	**90**	**90**	**90**	**94**	**90**	**91**

Baik Rata-Rata Buruk

Gambar 4.11 Tingkat Kesadaran Keamanan Menurut Jenis Kelamin

Pada Gambar 4.11 dari segi laki-laki, didapatkan skor 90 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai rata-rata di rentang 89 hingga 92. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 94 hingga 97 dengan rata-rata nilai 95. Dengan kata lain, kesadaran keamaan terkait isu *hardware* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Lalu pada Gambar 4.11 dari segi perempuan, didapatkan skor 91 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata dengan selisih 1 skor dibandingkan dengan laki-laki. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai rata-rata di rentang 90 hingga 94 yang lebih tinggi beberapa skor dibandingkan dengan laki-laki. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 96 hingga 98 dengan rata-rata nilai 97. Dengan kata lain, kesadaran keamaan terkait isu *hardware* sama seperti laki-laki dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih bisa ditingkatkan level dan nilai kesadarannya tersebut.

Di antara laki-laki dan perempuan, secara skor keseluruhan tidak terdapat perbedaan yang signifikan antara keduanya. Tetapi pada area fokus *hardware,* nilai perempuan lebih tinggi dibandingkan laki-laki walaupun pada beberapa aspek lain seperti dimensi *behavior* pada area fokus PIN/Password dan *software* nilai laki-laki lebih tinggi dibandingkan dengan perempuan.

4.2.2 Skor Kesadaran Keamanan Berdasarkan Usia

Fokus Area / Dimensi (Bobot)	Usia < 25 Tahun				Usia 25 - 34 Tahun				Usia ≥ 35 Tahun			
	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area
PIN/Password	87	92	87	**88**	92	96	93	**93**	90	93	91	**91**
Hardware	97	97	95	**96**	96	98	94	**95**	96	99	97	**97**
Software	89	91	87	**88**	92	96	93	**93**	88	92	87	**88**
Internet	83	88	84	**85**	89	94	93	**92**	83	94	93	**90**
Total Kesadaran/Dimensi	**89**	**92**	**88**	**89**	**92**	**96**	**93**	**94**	**89**	**95**	**92**	**92**

Baik Rata-Rata Buruk

Gambar 4.12 Tingkat Kesadaran Keamanan Menurut Usia

Pada Gambar 4.12 dari segi usia di bawah 25 tahun, didapatkan skor 89 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai rata-rata di rentang 88 hingga 92. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 95 hingga 97 dengan rata-rata nilai 96. Dengan kata lain, kesadaran keamaan terkait isu *hardware* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Lalu pada Gambar 4.12 dari segi usia 25 sampai 34 tahun, didapatkan skor 94 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Tetapi jika dilihat dari masing-masing dimensi terdapat satu dimensi yang dikategorikan ke dalam nilai Baik yaitu *attitude* dengan skor 96. Walaupun begitu, dimensi lainnya seperti *knowledge* dan *behavior* dikategorikan ke dalam nilai rata-rata dengan skor berurutan 92 dan 93. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 94 hingga 98 dengan rata-rata nilai 95. Dengan kata lain, kesadaran keamaan terkait isu *hardware* sama seperti usia di bawah 25 tahun dirasa sudah baik dan perlu dipertahankan di level tersebut,

sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software*, dan internet walaupun sudah cukup baik tetapi masih bisa ditingkatkan level dan nilai kesadarannya tersebut.

Kemudian pada Gambar 4.12 dari segi usia 35 tahun ke atas, didapatkan skor 92 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Tetapi jika dilihat dari masing-masing dimensi terdapat satu dimensi yang dikategorikan ke dalam nilai Baik yaitu *attitude* dengan skor 95. Walaupun begitu, dimensi lainnya seperti *knowledge* dan *behavior* dikategorikan ke dalam nilai rata-rata dengan skor berurutan 89 dan 92. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 96 hingga 99 dengan rata-rata nilai 97. Dengan kata lain, kesadaran keamaan terkait isu *hardware* sama seperti usia di bawah 25 tahun dan 25 sampai 34 tahun dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software*, dan internet walaupun sudah cukup baik tetapi masih bisa ditingkatkan level dan nilai kesadarannya tersebut.

Di antara 3 pembagian di atas, secara skor keseluruhan terdapat perbedaan yang terlihat dari skor kesadaran keamanan usia 25 sampai 34 tahun yang lebih tinggi 5 skor dibandingkan usia di bawah 25 tahun, sedangkan dengan usia 35 tahun ke atas hanya berbeda 2 skor saja. Ini disebabkan usia 25 sampai 34 tahun sudah matang dari segi pemikiran dan masih muda yang menyebabkan bisa lebih paham dengan apa yang harus dilakukan ketika menggunakan *e-wallet* dengan cepat dan tepat. Batasan dewasa awal muncul pada rentang usia 22 sampai 35 tahun dari segi pertumbuhan dan perkembangan pemikiran dan tindakan untuk mengambil sebuah peran dalam kehidupan (Martha, 2001). Pada dimensi *attitude*, hanya usia di bawah 25 tahun saja yang masuk kategori nilai rata-rata dibandingkan kategori usia yang lain. Ini bisa terjadi karena secara umur kategori 25 sampai 34 tahun dan 35 tahun ke atas lebih matang dan lebih bijak ketika melakukan sesuatu hal dengan berpikir terlebih dahulu konsekuensi jika melakukan hal tersebut.

4.2.3 Skor Kesadaran Keamanan Berdasarkan Lokasi

Fokus Area / Dimensi (Bobot)	Kabupaten				Kota			
	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area
PIN/Password	89	93	89	**90**	88	93	89	**90**
Hardware	97	98	95	**96**	95	96	95	**95**
Software	89	92	87	**89**	90	92	90	**90**
Internet	84	90	88	**87**	84	91	87	**87**
Total Kesadaran/Dimensi	**90**	**93**	**90**	**90**	**89**	**93**	**90**	**91**

Baik Rata-Rata Buruk

Gambar 4.13 Tingkat Kesadaran Keamanan Menurut Lokasi

Pada Gambar 4.13 dari segi kabupaten, didapatkan skor 90 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude*, maupun *behavior* juga memiliki nilai rata-rata di rentang 90 hingga 93. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 95 hingga 98 dengan rata-rata nilai 96. Dengan kata lain, kesadaran keamaan terkait isu *hardware* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software*, dan internet walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Lalu pada Gambar 4.13 dari segi kota, didapatkan skor 91 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude*, maupun *behavior* juga memiliki nilai rata-rata di rentang 89 hingga 93. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 95 hingga 96 dengan rata-rata nilai 95. Dengan kata lain, kesadaran

keamaan terkait isu *hardware* sama seperti laki-laki dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih bisa ditingkatkan level dan nilai kesadarannya tersebut.

Di antara lokasi kabupaten dan kota, secara skor keseluruhan tidak terdapat perbedaan yang signifikan antara keduanya karena hanya berselisih 1 skor saja. Tetapi pada area fokus *hardware,* kabupaten lebih tinggi dibandingkan kota sedangkan pada area fokus *software* kota lebih tinggi dibandingkan kabupaten. Walaupun keduanya hanya berselisih 1 skor saja antara area fokus *hardware* dan *software*. Untuk area fokus PIN/Password dan Internet memiliki skor yang sama persis antara kabupaten dan kota.

4.2.4 Skor Kesadaran Keamanan Berdasarkan Asal Daerah

Fokus Area \ Dimensi (Bobot)	Pulau Jawa				Luar Pulau Jawa			
	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area
PIN/Password	89	93	89	**90**	87	92	88	**89**
Hardware	97	98	95	**96**	96	97	95	**96**
Software	89	92	88	**89**	92	93	90	**91**
Internet	84	91	88	**87**	84	87	86	**86**
Total Kesadaran/Dimensi	**90**	**94**	**90**	**91**	**90**	**92**	**90**	**90**

Baik Rata-Rata Buruk

Gambar 4.14 Tingkat Kesadaran Keamanan Menurut Asal Daerah

Pada Gambar 4.14 dari segi pulau Jawa, didapatkan skor 91 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai rata-rata di rentang 90 hingga 94.

Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 95 hingga 98 dengan rata-rata nilai 96. Dengan kata lain, kesadaran keamaan terkait isu *hardware* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Lalu pada Gambar 4.14 dari segi luar pulau Jawa, didapatkan skor 90 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai Rata-Rata di rentang 90 hingga 92. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 95 hingga 97 dengan rata-rata nilai 96. Dengan kata lain, kesadaran keamaan terkait isu *hardware* sama seperti laki-laki dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih bisa ditingkatkan level dan nilai kesadarannya tersebut.

Di antara asal daerah pulau Jawa dan luar pulau Jawa, secara skor keseluruhan tidak terdapat perbedaan yang signifikan antara keduanya karena hanya berselisih 1 skor saja di mana pulau Jawa lebih tinggi dibandingkan luar pulau Jawa. Pada dimensi *attitude,* skor pulau Jawa lebih tinggi 2 skor dibandingkan luar pulau Jawa. Tetapi pada area fokus *software,* luar Pulau Jawa lebih tinggi 2 skor dibandingkan pulau Jawa. Walaupun skor area fokus lainnya seperti PIN/Password, *hardware,* dan internet lebih tinggi dari pulau Jawa dibandingkan luar pulau Jawa. Ini bisa disebabkan karena intensitas pemakaian *e-wallet* yang lebih tinggi di daerah Jabodetabek yang berada di pulau Jawa dibandingkan kota lain diluar pulau Jawa.

4.2.5 Skor Kesadaran Keamanan Berdasarkan Pendidikan Terakhir

Fokus Area / Dimensi (Bobot)	Belum Lulus Kuliah				Sudah Lulus Kuliah			
	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area
PIN/Password	87	92	87	**88**	91	95	92	**92**
Hardware	97	97	95	**96**	96	98	95	**96**
Software	89	91	87	**88**	90	95	91	**92**
Internet	83	88	85	**85**	86	94	92	**91**
Total Kesadaran/Dimensi	**89**	**92**	**89**	**89**	**91**	**96**	**93**	**93**

Baik Rata-Rata Buruk

Gambar 4.15 Tingkat Kesadaran Keamanan Menurut Pendidikan Terakhir

Pada Gambar 4.15 dari segi yang belum lulus kuliah, didapatkan skor 89 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai Rata-Rata di rentang 89 hingga 92. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 95 hingga 97 dengan rata-rata nilai 96. Dengan kata lain, kesadaran keamaan terkait isu *hardware* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Lalu pada Gambar 4.15 dari segi yang sudah lulus kuliah, didapatkan skor 93 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Tetapi pada salah satu dimensi yaitu *attitude* mendapatkan skor 96 yang dikategorikan nilai Baik walaupun dimensi *knowledge* dan *behavior* hanya mendapat nilai rata-rata dengan skor berurutan 91 dan 93. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang

nilai 95 hingga 98 dengan rata-rata nilai 96. Dengan kata lain, kesadaran keamaan terkait isu *hardware* sama seperti laki-laki dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih bisa ditingkatkan level dan nilai kesadarannya tersebut.

Di antara yang belum dan sudah lulus kuliah, secara skor keseluruhan cukup terlihat perbedaan yang signifikan antara keduanya karena berselisih sampai 4 skor di mana skor yang sudah lulus kuliah lebih tinggi dibandingkan yang belum lulus kuliah. Hal ini sudah sewajarnya karena semakin tinggi pendidikan seseorang maka seharusnya orang tersebut semakin waspada terhadap risiko pencurian data ketika menggunakan *e-wallet* dikarenakan lebih banyak ilmu yang sudah didapat dan diaplikasikan dalam kehidupan sehari-hari. Tingkat pendidikan seseorang mempengaruhi kinerja kedisiplinan dan kewaspadaan dalam menyelesaikan tugas dan tanggung jawabnya ketika beraktivitas (Putra, Suwendra, & Bagia, 2016). Pada dimensi *knowledge, attitude,* dan *behavior* skor yang sudah lulus kuliah lebih tinggi dibandingkan yang belum lulus kuliah dengan selisih secara berurutan 2 skor, 4 skor, dan 4 skor. Pada area fokus pun terjadi hal yang sama yaitu skor yang sudah lulus kuliah lebih tinggi dibandingkan yang belum lulus kuliah.

4.2.6 Skor Kesadaran Keamanan Berdasarkan Penghasilan Bulanan

Fokus Area / Dimensi (Bobot)	< 1 Juta per Bulan				≥ 1 Juta per Bulan			
	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area	Knowledge (30)	Attitude (20)	Behaviour (50)	Total Kesadaran/Fokus Area
PIN/Password	86	92	86	**87**	91	94	91	**92**
Hardware	97	97	94	**96**	97	98	96	**97**
Software	87	90	87	**88**	91	94	89	**91**
Internet	81	88	85	**84**	86	92	89	**89**
Total Kesadaran/Dimensi	**88**	**92**	**88**	**89**	**91**	**95**	**91**	**92**

Baik Rata-Rata Buruk

Gambar 4.16 Tingkat Kesadaran Keamanan Menurut Penghasilan Bulanan

Pada Gambar 4.16 dari segi yang penghasilan bulanannya di bawah Rp. 1.000.000, didapatkan skor 89 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Begitu pula jika dilihat dari masing-masing dimensi baik *knowledge, attitude,* maupun *behavior* juga memiliki nilai rata-rata di rentang 88 hingga 92. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori baik dengan rentang nilai 94 hingga 97 dengan rata-rata nilai 96. Dengan kata lain, kesadaran keamaan terkait isu *hardware* dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih ada peluang untuk ditingkatkan level dan nilai kesadarannya tersebut.

Lalu pada Gambar 4.16 dari segi yang penghasilan bulanannya Rp. 1.000.000 atau lebih, didapatkan skor 92 yang dalam penelitian ini dikategorikan ke dalam nilai rata-rata. Tetapi pada salah satu dimensi yaitu *attitude* mendapatkan skor 95 yang dikategorikan nilai Baik walaupun dimensi *knowledge* dan *behavior* hanya mendapat nilai rata-rata dengan skor 91. Dari keempat area fokus yang ada, hanya area fokus *hardware* yang mendapatkan kategori

baik dengan rentang nilai 96 hingga 98 dengan rata-rata nilai 97. Dengan kata lain, kesadaran keamaan terkait isu *hardware* sama seperti laki-laki dirasa sudah baik dan perlu dipertahankan di level tersebut, sedangkan ketiga area fokus lainnya seperti penggunaan PIN/password, *software,* dan internet walaupun sudah cukup baik tetapi masih bisa ditingkatkan level dan nilai kesadarannya tersebut.

Di antara yang penghasilan bulanannya di bawah Rp. 1.000.000 dan di Rp. 1.000.000 atau lebih, secara skor keseluruhan cukup terlihat perbedaan yang signifikan antara keduanya karena berselisih sampai 3 skor di mana skor yang penghasilan bulanannya Rp. 1.000.000 atau lebih ternyata skornya lebih tinggi dibandingkan yang penghasilan bulanannya di bawah Rp. 1.000.000. Hasil ini sangat wajar mengingat *e-wallet* memang merupakan uang hanya bentuknya digital bukan fisik. *E-wallet* sama seperti dompet fisik, hanya saja berupa digital yang digunakan untuk menyimpan informasi seperti nomor kartu kredit, e-cash, identitas pemilik, informasi kontak, informasi pengiriman atau penagihan termasuk alamat pelanggan dan informasi lain yang digunakan pada saat pembayaran (Junadi & Sfenrianto, 2015). Ketika seseorang memiliki penghasilan yang tinggi maka kewaspadaan dan penjagaan terhadap keuangannya pun akan meningkat untuk menghindari risiko yang bisa saja terjadi sewaktu-waktu seperti pencurian. Sebaliknya, untuk seseorang yang memiliki penghasilan yang rendah maka akan memiliki tingkat kewaspadaan dan penjagaan yang lebih rendah dikarenakan nominal gaji atau uang harus disimpan kecil. Gaji yang dimiliki seseorang mempengaruhi tanggung jawab seseorang karena keharusan memenuhi kebutuhannya, semakin tinggi kebutuhan maka semakin tinggi gaji yang harus dipertanggungjawabkan begitu pun sebaliknya (Pradana, 2014).

4.3 Kode Program untuk Regresi Linear Berganda

Melalui regresi linear berganda yang dihitung menggunakan RStudio dengan Bahasa Pemrograman R akan memudahkan proses pencarian faktor-faktor yang berpengaruh pada perbedaan tingkat kesadaran keamanan pengguna *e-wallet* di Indonesia seperti terlihat pada gambar-gambar di bawah.

```
#___data prep e wallet___#
#kode 1
library(gsheet)
dewal <-
gsheet2tbl("https://docs.google.com/spreadsheets/d/1r8DYY9OwvtKxV2DJ4oeuLvroEOq6ppB
BZ-c4gFsQbDA/edit?usp=sharing")
View(dewal)
summary(dewal)
str(dewal)
```

Gambar 4.17 Kode Program untuk Memanggil File Google Sheets yang Berisikan Data untuk Analisis

Pada Gambar 4.17 merupakan kode program untuk mengunduh terlebih dahulu Google Sheets sebagai tabel dari link yang dapat disebarkan melalui library *gsheet* menggunakan fungsi *gsheet2tbl*. Lalu, fungsi *view* digunakan untuk menampilkan data dari Google Sheets sebelumnya ke dalam RStudio. Kemudian, fungsi *summary* digunakan untuk menghasilkan hasil ringkasan dari berbagai fungsi *model fitting* dan fungsi *str* digunakan untuk menghasilkan secara ringkas struktur internal objek R, fungsi diagnosis dan alternatif untuk ringkasan.

```
#___variable desc e wallet___#
# id        no unik responden
# na        nilai total awareness per orang
# jk        jenis kelamin (perempuan = 1)
# us        usia/umur
# pd        pendidikan terakhir (sudah lulus kuliah = 1)
# inc       income/pemasukan dalam sebulan (< 1 jt = 1)
# pl        pulau (jawa = 1)
# ad        asal daerah kabupaten/kota (kota = 1)
```

Gambar 4.18 Deskripsi Nama Kolom dan Variabel yang Digunakan

Pada Gambar 4.18 merupakan penjelasan terkait singkatan variabel yang digunakan untuk analisis regresi linear berganda.

```
#___multiple linear regression e wallet___#
#kode 1 unstandardized
mlr <- lm(na ~  jk + us + ad + pl + pd + inc, data = dewal)
print(mlr)
summary(mlr)

#kode 2 standardized
mlr.sd <- lm(scale(na) ~  scale(jk) + scale(us) + scale(ad) + scale(pl) + scale(pd)
+ scale(inc), data = dewal)
print(mlr.sd)
summary(mlr.sd)
```

Gambar 4.19 Kode Program untuk Analisis Regresi Linear Berganda

Pada Gambar 4.19 merupakan kode program untuk melakukan proses analisis regresi linear berganda. Pada kode program yang pertama merupakan kode untuk analisis regresi linear berganda yang belum di standarisasi nilai *dependent variable* dan *independent variable* yang

memberi tahu seberapa banyak perubahan dalam *dependent variable* (Y) yang diprediksi terjadi per unit perubahan dalam *independent variable* (X). Lalu, pada kode program yang kedua merupakan kode untuk analisis regresi linear berganda yang sudah di standarisasi nilai *dependent variable* dan *independent variable* dengan standar deviasi yang memberi tahu seberapa banyak perubahan dalam *dependent variable* (Y) yang diprediksi terjadi per unit perubahan dalam *independent variable* (X).

Ketika kode program tersebut dijalankan pada Rstudio akan menyajikan beragam informasi seperti nilai koefisien dan tingkat signifikan pada suatu variabel. Melalui kode program ini didapatkan nilai estimasi, nilai standar eror, tingkat pengaruh variabel yang mempengaruhi skor kesadaran keamanannya, dan lain sebagainya. Selain itu terdapat fungsi *print* yang digunakan untuk menampilkan hasil analisis regresi linear berganda dan fungsi *summary* yang digunakan menghasilkan hasil ringkasan dari berbagai fungsi *model fitting.*

Pada Gambar 4.20 merupakan kode program untuk menguji *outlier* pada data yang digunakan. *Outlier* adalah kasus atau data yang memiliki karakteristik unik yang terlihat sangat berbeda jauh dari observasi-observasi lainnya dan muncul dalam bentuk nilai ekstrim baik untuk sebuah variabel tunggal atau kombinasi (Ghozali, 2009). Pada kode program pertama berfungsi untuk membuat *plot* matriks sebar yang ditingkatkan, termasuk tampilan univariat pada diagonal dan berbagai garis yang dipasang. Lalu, kode program yang kedua dan ketiga digunakan untuk menghasilkan nilai dari sisa bagi dengan standar deviasi yang pada kode kedua *range* di antara -3 sampai 3, sedangkan kode ketiga range di antara -2,5 sampai 2,5. Dari kode tersebut akan menghasilkan data yang kemungkinan *outlier*. Selanjutnya kode keempat, kelima, dan keenam merupakan kode untuk mencari *outlier* melalui Bonferroni *p-values, high leverage,* dan *Cook's distance.*

Lalu, kode ketujuh berfungsi untuk membuat *plot* "gelembung" dari *studentized residuals* versus *hat values* dengan area lingkaran yang mewakili pengamatan yang sebanding dengan nilai *Cook's distance*. Dari *plot* ini, dapat dihasilkan *outlier* akhir dengan membandingkan 3 cara yang berbeda untuk mencari *outlier* tersebut agar mendapatkan hasil yang akurat. Kemudian, kode kedelapan berfungsi untuk memberikan pengaruh dari indeks *plot* dan diagnostik terkait untuk mode regresi. Terakhir, kode kesembilan berfungsi untuk membandingkan *residuals* dengan *fitted values* untuk menguji homoskedastisitas. Homoskedastisitas berarti bahwa varian dari error bersifat konstan (Mokosolang, Prang, & Mananohas, 2015).

Terdapat 5 *outlier* yang ditemukan yaitu data ke 113, 122, 228, 262, dan 295. *Outlier* tersebut tidak akan dimasukkan ke dalam perhitungan analisis regresi linear berganda untuk menghindari perubahan nilai yang jauh dikarenakan *outlier* tersebut dan menambah keakuratan hasil analisis.

```
#Diagnostic untuk menguji outlier
#kode 1
library(car)
scatterplotMatrix(~ na + jk + us + ad + pl + pd + inc, data = dewal)

#kode 2, studentized residuals range -3,0,3
res.std <- rstandard(mlr)
plot(res.std, ylab="Standardized Residual", ylim=c(-3.5,3.5))
abline(h =c(-3,0,3), lty = 2)
index <- which(res.std > 3 | res.std < -3)
text(index-20, res.std[index] , labels = dewal$id[index])
print(index)
print(dewal$id[index])

#kode 3, studentized residuals range -2.5,0,2.5
plot(res.std, ylab="Standardized Residual", ylim=c(-3.5,3.5))
abline(h =c(-2.5,0,2.5), lty = 2)
index <- which(res.std > 2.5 | res.std < -2.5)
text(index-20, res.std[index] , labels = dewal$id[index])
print(index)
print(dewal$id[index])

#kode 4, Bonferroni p-values for testing outlier
outlierTest(mlr)

#kode 5, detecting points with high leverage
library(faraway)
h <- influence(mlr)$hat
halfnorm(influence(mlr)$hat, ylab = "leverage")

#kode 6, the cut of value for cook's distance
cutoff <- 4/((nrow(dewal)-length(mlr$coefficients)-2))
plot(mlr, which = 4, cook.levels = cutoff)

#kode 7, cook's distance, standardized residuals, and leverage in the same plot
influencePlot(mlr, main="Influence Plot", sub="Circle size is proportional to
Cook's Distance" )

#kode 8, for diagnostic plots to identify influential points
infIndexPlot(mlr)


#kode 9, residual vs. fitted value plot for Homoscedasticity
plot(mlr$resid ~ mlr$fitted.values)
abline(h = 0, lty = 2)
```

Gambar 4.20 Kode Program untuk Diagnosis *Outliers*

Pada Gambar 4.21 kedua baris program selanjutnya merupakan kode untuk analisis regresi linear berganda yang belum di standarisasi dan yang sudah di standarisasi nilai *dependent variable* dan *independent* tanpa *outlier* tersebut yang sebelumnya sudah didapatkan melalui proses diagnostik. Selain itu, terdapat fungsi tambahan dari kode program sebelumnya

yaitu fungsi *vif* yang digunakan untuk mendapatkan nilai VIF (*Variance Inflation Factor)* untuk setiap *independent variable.*

```
#___hasil regresi terbaru setelah diagnostic tanpa outlier___#
#kode 1 unstandardized
library(car)
mlr2 <- lm(na ~  jk + us + ad + pl + pd + inc, data = dewal[-
c(113,122,228,262,295),])
print(mlr2)
summary(mlr2)
vif(mlr2)

#kode 2 standardized
mlr2.sd <- lm(scale(na) ~  scale(jk) + scale(us) + scale(ad) + scale(pl) +
scale(pd) + scale(inc), data = dewal[-c(113,122,228,262,295),])
print(mlr2.sd)
summary(mlr2.sd)
vif(mlr2.sd)
```

Gambar 4.21 Kode Program untuk Analisis Regresi Linear Berganda Tanpa *Outlier*

Pada Gambar 4.22 baris pertama merupakan kode program untuk menghitung rata-rata nilai VIF (*Variance Inflation Factor*) dari keseluruhan *independent variable* pada analisis regresi linear berganda. Kemudian, pada baris kedua merupakan kode program untuk mencari nilai *Ramsey RESET Test*. *Ramsey RESET Test* merupakan uji spesifikasi umum untuk model regresi linear yang dikembangkan oleh James B. Ramsey. Kata *RESET* merupakan singkatan dari *Regression Equation Specification Error Test* atau terjemahan dalam Bahasa Indonesia adalah Uji Kesalahan Spesifikasi Persamaan Regresi.

```
#mean VIF
#kode 1
meanvif <- (1.016318+1.746781+1.060743+1.079427+1.853339+1.425274)/6
print(meanvif)

#ramsey reset test
#kode 2
library(lmtest)
resettest(mlr2.sd, power = 2:3, type = c("fitted", "regressor",
"princomp"), data = dewal[-c(113,122,228,262,295),])
```

Gambar 4.22 Perhitungan Untuk Mencari Rata-Rata Nilai VIF dan Nilai Ramsey Reset Test

Pada Gambar 4.23 merupakan kode program untuk memvisualisasikan skor kesadaran keamanan terhadap faktor yang mempengaruhinya pada penelitian ini yaitu jenis kelamin, usia, lokasi kabupaten/kota, asal daerah Pulau Jawa dan luar Jawa, pendidikan terakhir, dan penghasilan bulanan dari pengguna *e-wallet* di Indonesia. Terdapat 2 *library* yang digunakan yaitu *library jtools* dan *ggplot2*. *Library jtools* adalah kumpulan alat agar lebih efisien dalam

memahami dan berbagi hasil terutama dalam menganalisis regresi yang di dalamnya terdapat sejumlah fungsi untuk keperluan statistik dan pemrograman, sedangkan *library ggplot2* adalah sebuah alat untuk membuat grafik dengan kita yang memberikan data, memberi tahu *ggplot2* cara memetakan variabel ke estetika, primitif grafis apa yang digunakan, dan menangani detailnya. Lalu, fungsi *effect plot* yang digunakan untuk membuat visualisasi dalam bentuk *plot* yang fungsinya terdapat dalam *library jtools* untuk memudahkan penjelasan terkait pengaruh faktor-faktor demografis yang sudah disebutkan terhadap skor kesadaran keamanan pengguna E-Wallet di Indonesia. Kemudian, di dalam fungsi *effect plot* terdapat fungsi lain yaitu *ylim* yang digunakan untuk membatasi skala skor kesadaran keamanan yang divisualisasikan yang terdapat dalam *library ggplot2.*

```
#___visualisasi faktor___#
library(jtools)
library(ggplot2)
effect_plot(mlr2, pred = jk, interval = TRUE, y.label = "Skor Kesadaran Keamanan",
x.label = "Perempuan") + ylim(85,95)
effect_plot(mlr2, pred = us, interval = TRUE, y.label = "Skor Kesadaran Keamanan",
x.label = "Usia") + ylim(85,95)
effect_plot(mlr2, pred = ad, interval = TRUE, y.label = "Skor Kesadaran Keamanan",
x.label = "Kota") + ylim(85,95)
effect_plot(mlr2, pred = pl, interval = TRUE, y.label = "Skor Kesadaran Keamanan",
x.label = "Pulau Jawa") + ylim(85,95)
effect_plot(mlr2, pred = pd, interval = TRUE, y.label = "Skor Kesadaran Keamanan",
x.label = "Pendidikan Tinggi") + ylim(85,95)
effect_plot(mlr2, pred = inc, interval = TRUE, y.label = "Skor Kesadaran Keamanan",
x.label = "Penghasilan Bulanan < Rp1.000.000") + ylim(85,95)
```

Gambar 4.23 Visualisasi Faktor-Faktor yang Berpengaruh

4.4 Hasil Regresi Linear Berganda

Dari hasil analisis regresi linear berganda yang bertujuan untuk mencari faktor-faktor demografis yang berpengaruh pada perbedaan tingkat kesadaran keamanan pengguna *e-wallet* di Indonesia disajikan pada Tabel 4.2.

Tabel 4.2 Hasil Regresi Linear Berganda atas
Skor Kesadaran Keamanan Pengguna E-Wallet di Indonesia

Jenis Kelamin	**-0.725**
Perempuan	**-0.042**
	(0.052)
Usia	**-0.023**
	-0.024
	(0.068)
Asal Daerah	**-0.211**
Kota	**-0.012**
	(0.053)
Pulau	**-1.160**
Jawa	**-0.050**
	(0.053)
Pendidikan	**2.496** *
Sudah lulus kuliah	**0.139**
	(0.070)
Penghasilan Bulanan	**-2.652** *
Kurang dari 1 juta rupiah	**-0.151**
	(0.061)
Constant/Intercept	93.314 ***
	6.584e-16
	(0.051)
R^2	**0.057**
Highest VIF	**1.853**
Mean VIF	**1.364**
Ramsey RESET Test	**0.775**
Observation	**365**

Catatan: Angka pada baris pertama adalah unstandardized estimate, baris kedua adalah standardized estimate (beta), dan baris ketiga adalah robust standard error; '***' p < 0.001, '**' p<0.01, '*' p<0.05, '.' p<0.1, ' ' p<1.

Dari hasil diagnosis pada iterasi awal, ditemukan lima buah *outliers* dan *influential cases* yang tidak disertakan pada iterasi berikutnya sehingga tersisa 365 responden yang menjadi model akhir di analisis regresi ini. Faktor yang memiliki pengaruh paling besar yaitu penghasilan bulanan dan diikuti oleh pendidikan terakhir. Apabila semua faktor lain bernilai sama, maka pengguna *e-wallet* yang memiliki penghasilan bulanan kurang dari 1 juta rupiah akan memiliki skor 2,6 poin lebih rendah dibandingkan yang berpenghasilan 1 juta ke atas per

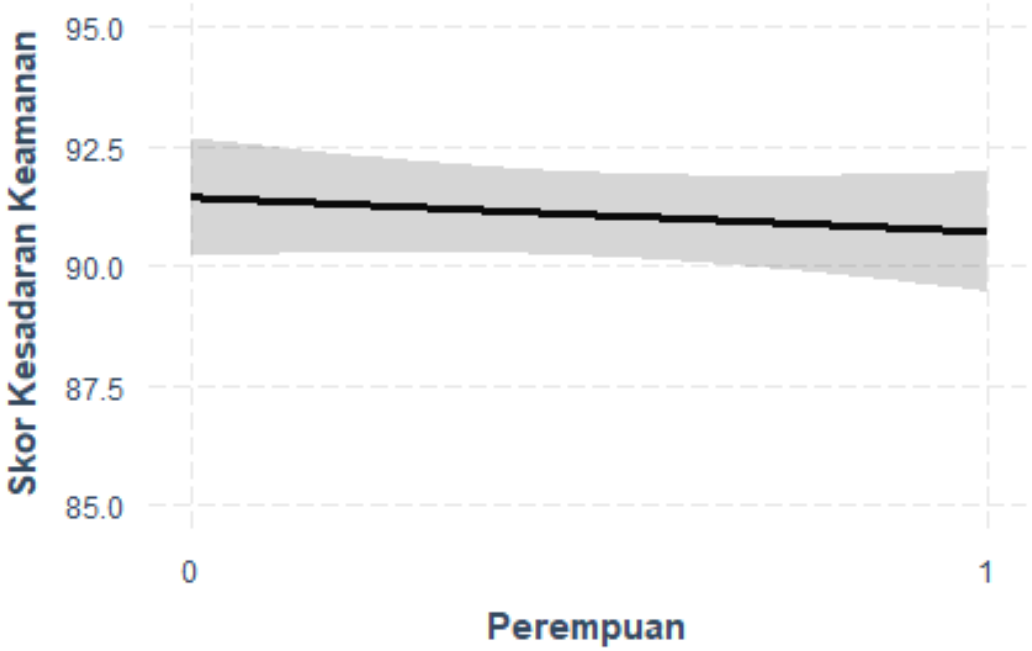
bulannya. Begitu pula dengan pendidikan terakhir, pengguna *e-wallet* yang memiliki pendidikan tinggi atau sudah lulus kuliah memiliki skor sekitar 2,5 poin lebih tinggi dibandingkan dengan yang tidak mengenyam atau belum menamatkan pendidikan di perguruan tinggi jika semua faktor dianggap konstan.

Sementara itu, dari sisi faktor lain seperti jenis kelamin, usia, dan lokasi baik asal daerah maupun pulau dalam penelitian ini tidak ditemukan perbedaan signifikan dari sisi skor kesadaran keamanannya. Pada faktor jenis kelamin, pengguna perempuan memiliki skor 0,7 poin lebih rendah dibandingkan laki-laki. Selanjutnya, pada faktor usia semakin muda pengguna maka akan memiliki skor 0,02 skor lebih rendah untuk setiap 1 tahun perbedaaan usianya. Lalu, pada faktor asal daerah pengguna yang tinggal di kota memiliki skor 0,2 lebih rendah dibandingkan yang tinggal di kabupaten. Kemudian, pada faktor pulau pengguna yang tinggal di Pulau Jawa memiliki skor 1,2 poin lebih rendah dibandingkan pengguna yang tinggal di luar Pulau Jawa meliputi Sumatera, Kalimantan, Sulawesi, dan lainnya.

R squared (R^2) merupakan nilai pengaruh yang diberikan *independent variable* yaitu jenis kelamin, usia, pendidikan, penghasilan, asal daerah, dan pulau terhadap *dependent variable* yaitu nilai kesadaran secara simultan atau bersama-sama yang yaitu sebesar 0,057 pada penelitian ini. Lalu, *highest dan mean VIF* secara berurutan adalah nilai terbesar *Variance Inflation Factor* (VIF) yang diperoleh dari masing-masing *independent variable* dan rata-rata nilai VIF dari masing-masing *independent variable* untuk uji multikolinearitas. Kemudian, *Ramsey RESET Test* adalah nilai dari uji statistik yang dikenal dengan Uji *Ramsey Regression Equation Spesification Error Test.* Sedangkan *observation* adalah jumlah data responden yang diproses pada analisis regresi linear berganda yang dilakukan.

4.4.1 Visualisasi Efek Faktor Jenis Kelamin

Dari hasil analisis regresi linear berganda faktor jenis kelamin, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.24.

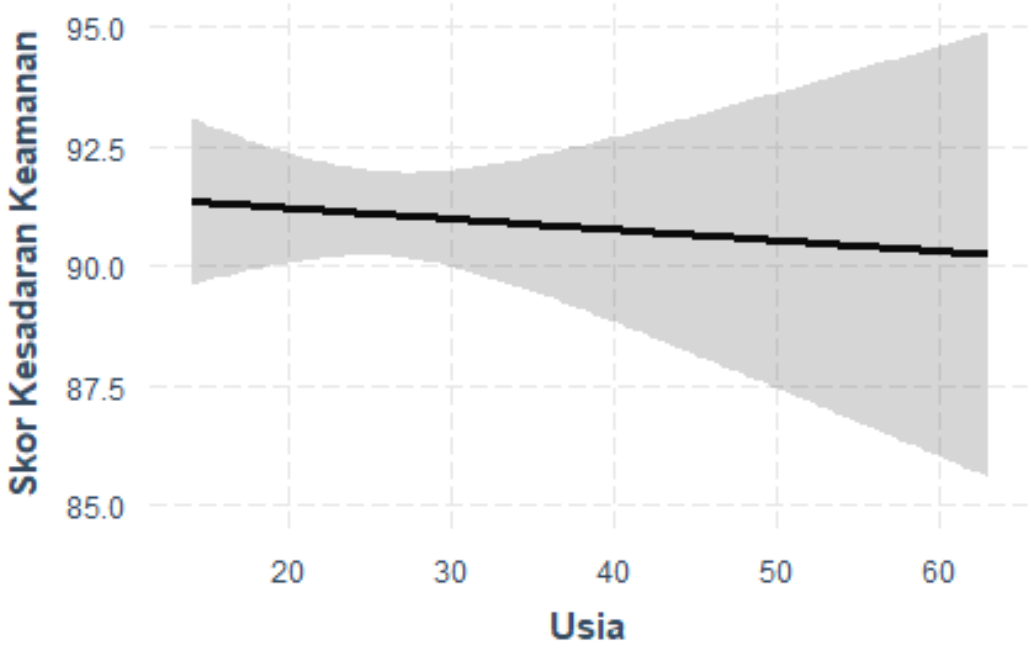


Gambar 4.24 Pengaruh Faktor Jenis Kelamin

Dari Gambar 4.24, pengaruh dari faktor jenis kelamin tidak terlalu terlihat atau tidak signifikan sesuai dengan Tabel 4.2 sebelumnya walaupun ada perbedaaan sedikit. Untuk setiap pengguna E-Wallet dengan jenis kelamin perempuan akan memiliki skor 0,7 poin lebih rendah dibandingkan pengguna yang dengan jenis kelamin laki-laki.

4.4.2 Visualisasi Efek Faktor Usia

Dari hasil analisis regresi linear berganda faktor usia atau umur, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.25.

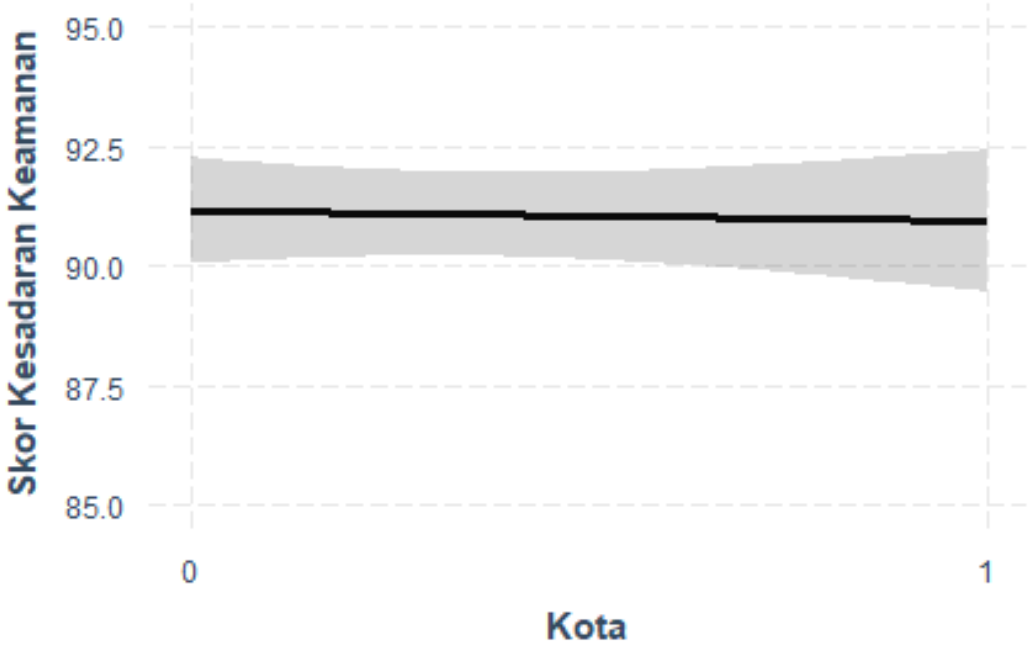


Gambar 4.25 Pengaruh Faktor Usia

Dari Gambar 4.25, pengaruh dari faktor usia terlihat ada perbedaan untuk setiap skor kesadaran keamanan walaupun tidak signifikan sesuai dengan Tabel 4.2. Semakin tua usia pengguna E-Wallet tersebut maka akan turun skor kesadaran keamanannnya sebanyak 0,02 poin setiap 1 tahun lebih tua. Sebaliknya, semakin muda usia pengguna E-Wallet tersebut maka akan naik skor kesadaran keamanannya sebanyak 0,02 poin setiap 1 tahun lebih muda.

4.4.3 Visualisasi Efek Faktor Asal Daerah

Dari hasil analisis regresi linear berganda faktor asal daerah yaitu kabupaten dan kota, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.26.

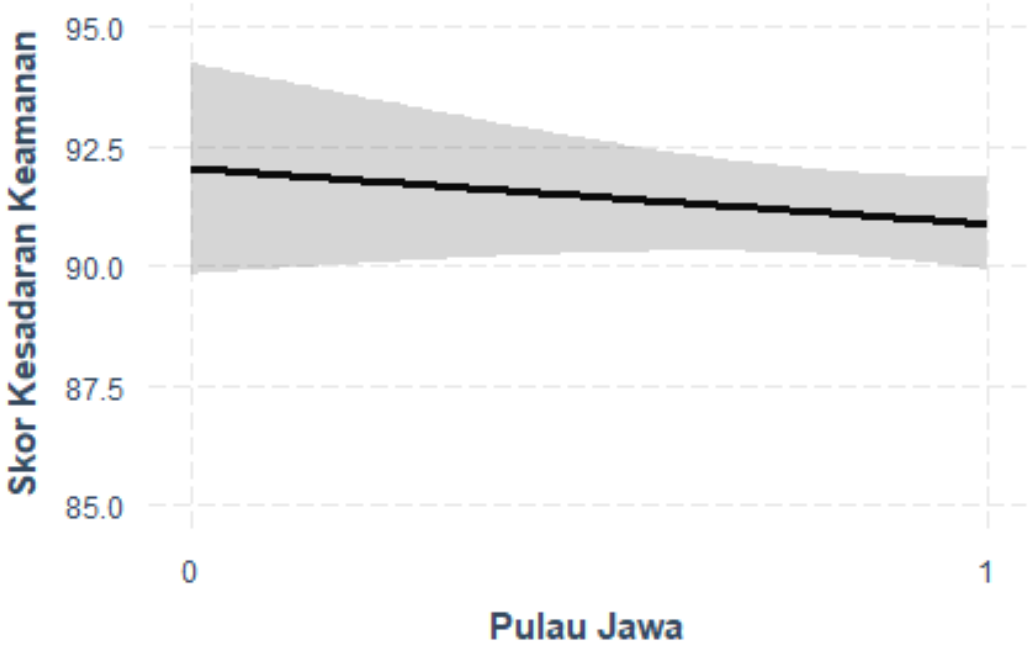


Gambar 4.26 Pengaruh Faktor Asal Daerah

Dari Gambar 4.26, pengaruh dari faktor asal daerah terlihat ada perbedaan untuk setiap skor kesadaran keamanan walaupun tidak signifikan sesuai dengan Tabel 4.2. Untuk setiap pengguna E-Wallet yang tinggal di daerah kota akan memiliki skor 0,2 poin lebih rendah dibandingkan pengguna yang tinggal di daerah kabupaten. Sebaliknya, setiap pengguna E-Wallet yang tinggal di daerah kabupaten akan memiliki skor 0,2 poin lebih tinggi dibandingkan dengan pengguna yang tinggal di daerah kota.

4.4.4 Visualisasi Efek Faktor Pulau

Dari hasil analisis regresi linear berganda faktor asal daerah yaitu Pulau Jawa dan luar Pulau Jawa, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.27.

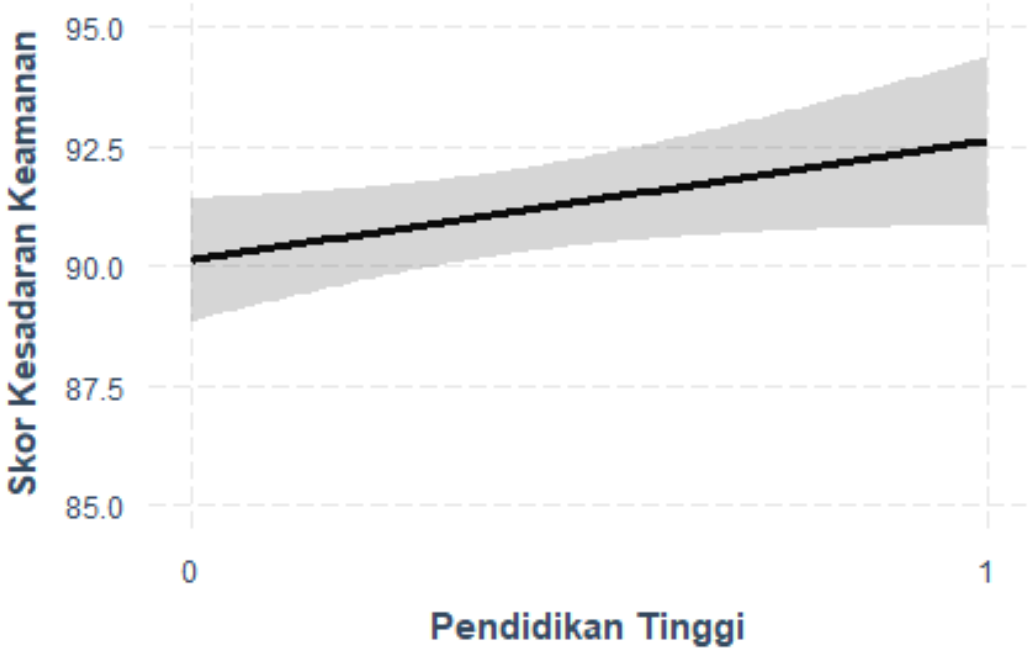


Gambar 4.27 Pengaruh Faktor Pulau

Dari Gambar 4.27, pengaruh dari faktor pulau cukup terlihat ada perbedaan untuk setiap skor kesadaran keamanan walaupun tidak signifikan sesuai dari hasil analisis pada Tabel 4.2. Untuk setiap pengguna E-Wallet yang tinggal di Pulau Jawa akan memiliki skor 1,2 poin lebih rendah dibandingkan pengguna yang tinggal di daerah luar Pulau Jawa. Sebaliknya, setiap pengguna E-Wallet yang tinggal di daerah luar Pulau Jawa akan memiliki skor 1,2 poin lebih tinggi dibandingkan dengan pengguna yang tinggal di Pulau Jawa.

4.4.5 Visualisasi Efek Faktor Pendidikan

Dari hasil analisis regresi linear berganda faktor pendidikan terakhir yang dimiliki oleh pengguna, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.28.

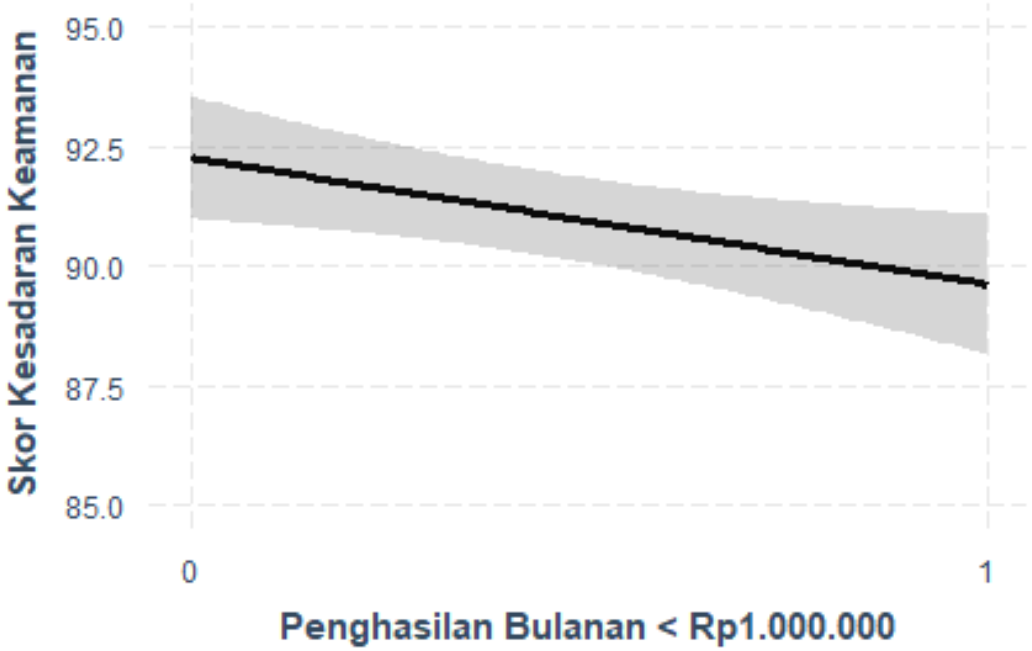


Gambar 4.28 Pengaruh Faktor Pendidikan Terakhir

Dari Gambar 4.28, pengaruh dari faktor pendidikan terakhir sangat terlihat perbedaannya untuk setiap skor kesadaran keamanan karena sesuai dari hasil analisis pada Tabel 4.2 faktor ini sangat berpengaruh secara signifikan. Untuk setiap pengguna E-Wallet yang memiliki pendidikan tinggi atau sudah lulus kuliah akan memiliki skor 2,5 poin lebih tinggi dibandingkan pengguna yang memiliki pendidikan rendah atau belum lulus kuliah. Sebaliknya, setiap pengguna E-Wallet yang memiliki pendidikan rendah atau belum lulus kuliah akan memiliki skor 2,5 poin lebih rendah dibandingkan dengan pengguna yang memiliki pendidikan tinggi atau sudah lulus kuliah.

4.4.6 Visualisasi Efek Faktor Penghasilan Bulanan

Dari hasil analisis regresi linear berganda faktor penghasilan bulanan yang dimiliki oleh pengguna, maka di visualisasikan ke dalam bentuk *plot* agar terlihat jelas pengaruhnya terhadap skor kesadaran keamanan yang disajikan pada Gambar 4.29.



Gambar 4.29 Pengaruh Faktor Penghasilan Bulanan

Dari Gambar 4.29, pengaruh dari faktor penghasilan bulanan sangat terlihat perbedaannya untuk setiap skor kesadaran keamanan karena sesuai dari hasil analisis pada Tabel 4.2 faktor ini sangat berpengaruh secara signifikan. Untuk setiap pengguna *e-wallet* yang memiliki penghasilan bulanan kurang dari 1 juta rupiah akan memiliki skor 2,6 poin lebih rendah dibandingkan yang berpenghasilan 1 juta ke atas per bulannya. Sebaliknya, setiap pengguna *e-wallet* yang memiliki penghasilan bulanan 1 juta ke atas akan memiliki skor 2,6 poin lebih tinggi dibandingkan yang berpenghasilan kurang dari 1 juta per bulannya. Hal ini sangat wajar karena semakin besar uang yang disimpan atau digunakan oleh seseorang, maka orang tersebut akan memiliki tingkat pengawasan dan penjagaan yang lebih untuk menghindari hal yang tidak diinginkan ketika bertransaksi menggunakan uang tersebut, salah satunya *e-wallet*.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian ini yang telah dilakukan, maka dapat didapati hasil besaran pengetahuan tentang keamanan yaitu bernilai 90 dari nilai maksimal 100 yang berada pada tingkatan rata-rata berdasarkan Gambar 4.10. sebelumnya pada bagian dimensi *knowledge*. Lalu, tingkat kesadaran keamanan atau *security awareness* pengguna *e-wallet* di Indonesia yaitu berada pada tingkatan rata-rata berdasarkan nilai kesadaran total yang ada pada Gambar 4.10. sebelumnya yaitu bernilai 91 dari nilai maksimal 100. Dengan hasilnya berada pada tingkatan rata-rata, memberikan dampak kepada kebiasaan pengguna yang dinilai sudah cukup baik berdasarkan pertanyaan yang dijawab pada kuesioner tetapi masih dapat ditingkatkan kembali di beberapa bagian, terutama pada area fokus PIN/password, *software* dan internet yang cukup jauh tertinggal jika dibandingkan area fokus *hardware.* Pada ketiga area tersebut, perlu dilakukan upaya-upaya khusus dalam bentuk edukasi pengguna untuk meningkatkan kesadaran keamanan informasi pengguna *e-wallet* untuk menghindari ancaman yang bisa saja terjadi sewaktu-waktu.

Selain itu, penelitian ini juga menemukan perbedaan tingkat kesadaran keamanan pengguna *e-wallet* di Indonesia berdasarkan faktor demografis seperti jenis kelamin, usia, lokasi baik berdasarkan pulau maupun kabupaten/kota, penghasilan bulanan dan tingkat pendidikan. Pengguna *e-wallet* dengan penghasilan rendah memiliki tingkat kesadaran keamanan yang lebih rendah berdasarkan penelitian yang telah dilakukan. Kemudian, pengguna *e-wallet* dengan latar belakang pendidikan tinggi memiliki tingkat kesadaran keamanan yang lebih tinggi dibandingkan mereka yang belum menamatkan atau tidak mengenyam pendidikan tinggi berdasarkan penelitian yang telah dilakukan. Adapun terkait faktor lain seperti jenis kelamin, usia, dan lokasi, walaupun ada perbedaan tetapi tidak signifikan antar kelompok pengguna *e-wallet* yang berbeda dalam penelitian ini. Hasil dari penelitian ini diharapkan dapat berguna untuk menjadi sebuah acuan untuk melakukan penelitian serupa dengan fokus yang berbeda ke depannya.

5.2 Saran

Masih terdapat beberapa batasan atau kekurangan yang ada pada penelitian ini, seperti pertanyaan yang digunakan untuk menghitung skor kesadaran keamanan masih perlu ditingkatkan baik dari sisi kuantitas atau jumlahnya maupun kualitas misal dengan melibatkan pakar baik dari sisi keamanan maupun dari sisi penyedia layanan *e-wallet* dalam proses penyusunannya. Kemudian karakteristik responden yang masih cenderung homogen, baik dari sisi usia maupun lokasi juga berpotensi menyebabkan nilai kesadaran pengguna yang perlu kehati-hatian lebih jika akan dilakukan proses generalisasi ke seluruh pengguna *e-wallet* di Indonesia.

DAFTAR PUSTAKA

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. *Jurnal Sistem Informasi Bisnis*, *8*(2), 115. https://doi.org/10.21456/vol8iss2pp115-122

Al-Shehri, Y. (2012). Information Security Awareness and Culture. *British Journal of Arts and Social Sciences*.

Andika, M., Listiawati, R., Novitasari, & Vidyasari, R. (2019). *Analisa Pengaruh Daya Tarik Promosi, Persepsi Kemudahan, Persepsi Manfaat, Persepsi Keamanan Terhadap Minat Penggunaan E-Wallet*. *18*(2), 126–134.

Astuti, R. K. (n.d.). Waspada! Akun Dompet Digital Rawan Dibobol Hacker. Retrieved November 2, 2020, from https://www.cnbcindonesia.com/tech/20200104173743-37-127676/waspada-akun-dompet-digital-rawan-dibobol-hacker

Bada, M., Sasse, A. M., & Nurse, J. R. C. (n.d.). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*

Badan Pusat Statistik. (2019). Statistik Indonesia 2019. *BPS, 2019 (Indonesian Statistics)*, Jakarta: Badan Pusat Statistik.

Barlian, E. (2016). Metodologi Penelitian Kualitatif dan Kuantitatif. *Sukabina Press*, 247.

Batmetan, J. R., Kariso, B., Moningkey, M., & Tumembow, A. (2018). *Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi*. https://doi.org/10.31219/OSF.IO/CAHZR

Bosamia, M., & Patel, D. (2019). Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. *International Journal of Computer Sciences and Engineering*, *7*(1), 810–817. https://doi.org/10.26438/ijcse/v7i1.810817

Daftar 50 Website & Aplikasi E-Commerce di Indonesia 2019. (n.d.). Retrieved October 22, 2020, from https://iprice.co.id/insights/mapofecommerce/

Etikan, I. (2016a). Comparision of Snowball Sampling and Sequential Sampling Technique. *Biometrics & Biostatistics International Journal*, *3*(1), 1–2. https://doi.org/10.15406/bbij.2016.03.00055

Etikan, I. (2016b). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

Feldman, R. (1999). *Understanding Psychology. 5th ed. Boston, River Ridge, IL: McGraw-Hill College*.

Ghozali, I. (2009). Aplikasi Multivariate Lanjutan Dengan Program SPSS. In *Badan Penerbit*

Universitas Diponegoro.

Gio, P. U., & Effendie, A. R. (2018). *Belajar Bahasa Pemrograman R*. https://doi.org/10.31227/osf.io/ktmy2

Hansche, S. (2001). Designing a security awareness program: Part 1. *Information Systems Security*, *9*(6), 1–9. https://doi.org/10.1201/1086/43298.9.6.20010102/30985.4

Harlan, J. (2018). Analisis Regresi Linear. In *Journal of Chemical Information and Modeling* (Vol. 53).

Heckathorn, D. D. (2011). Comment: Snowball versus Respondent-Driven Sampling. *Sociological Methodology*, *41*(1), 355–366. https://doi.org/10.1111/j.1467-9531.2011.01244.x

Hsu, H.-Y., & Wang, S.-K. (2017). Integrating Technology: Using Google Forms to Collect and Analyze Data. *Science Scope*, *040*(08), 64–67. https://doi.org/10.2505/4/ss17_040_08_64

Iskandar. (n.d.). Aura Kasih Kehilangan Rp 11 Juta di Gopay, Ini Penjelasan Gojek - Tekno Liputan6.com. Retrieved June 24, 2020, from https://www.liputan6.com/tekno/read/4113650/aura-kasih-kehilangan-rp-11-juta-di-gopay-ini-penjelasan-gojek

Janna, N. M. (2020). *Variabel dan Skala Pengukuran Statistik*. 1–8. Retrieved from https://doi.org/10.31219/osf.io/8326r

Jeff Smith, H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/41409970

Junadi, & Sfenrianto. (2015). A Model of Factors Influencing Consumer's Intention to Use E-payment System in Indonesia. *Procedia Computer Science*, *59*(Iccsci), 214–220. https://doi.org/10.1016/j.procs.2015.07.557

Kamaliah, A. (n.d.). Awas! Penjahat di Indonesia Incar Dompet Digital. Retrieved November 2, 2020, from https://inet.detik.com/security/d-4740593/awas-penjahat-di-indonesia-incar-dompet-digital

Kanimozhi. G, K. . K. (2017). Security Aspects of Mobile Based E Wallet. *Ijritcc.Com*, 1223–1228. Retrieved from https://ijritcc.com/index.php/ijritcc/article/view/931

Kencana Sari, P., & Candiwan. (2014). Measuring information security awareness of Indonesian smartphone users. *Telkomnika (Telecommunication Computing Electronics and Control)*, *12*(2), 493–500. https://doi.org/10.12928/TELKOMNIKA.v12i2.2015

Khadijah, C. (2019). Transformasi perpustakaan untuk generasi millenial menuju revolusi industri 4.0. *IQRA`: Jurnal Ilmu Perpustakaan Dan Informasi (e-Journal)*, *12*(2), 59. https://doi.org/10.30829/iqra.v12i2.3983

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kunicki, Z. J., Zambrotta, N. S., Tate, M. C., Surrusco, A. R., Risi, M. M., & Harlow, L. L. (2019). Keep Your Stats in the Cloud! Evaluating the Use of Google Sheets to Teach Quantitative Methods. *JOURNAL OF STATISTICS EDUCATION*, *27*(3), 188–197. https://doi.org/10.1080/10691898.2019.1665485

Laudon, Kenneth C., & Traver, C. G. (2011). *E-Commerce 2011. 7th ed. Harlow: Pearson Education Limited*.

Martha, R. (2001). Human Development: Children, Youth, and Adult Development and the Effect of Child Maltreatment on Human Development. *Barkeley: CalSWEC University of California*.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2016.11.065

Michener, H., & Delamater, J. (1994). *Michener HA, Delamater JD. Social psychology. 3rd ed. Orlando, Florida: Harcourt Brace College Publishers*.

Mokosolang, C., Prang, J., & Mananohas, M. (2015). Analisis Heteroskedastisitas Pada Data Cross Section dengan White Heteroscedasticity Test dan Weighted Least Squares. *D'CARTESIAN*, *4*(2), 172. https://doi.org/10.35799/dc.4.2.2015.9056

Nugroho, A. (n.d.). NEWS : Tiga Serangan yang Dipakai untuk Bobol Dompet Digital. Retrieved November 2, 2020, from https://cyberthreat.id/read/4643/Tiga-Serangan-yang-Dipakai-untuk-Bobol-Dompet-Digital

Pradana, O. (2014). PENGARUH MOTIVASI KERJA DAN KOMITMEN ORGANISASIONAL TERHADAP KINERJA KARYAWAN (Studi pada karyawan bagian HRD PT. Arthawena Sakti Gemilang Malang). *Jurnal Administrasi Bisnis S1 Universitas Brawijaya*, *7*(2), 78924.

Putra, I. W. I., Suwendra, I. W., & Bagia, I. W. (2016). *Pengaruh Tingkat Pendidikan dan Disiplin Kerja Terhadap Kinerja Karyawan*. *4*(1).

Ridhoi, M. A. (n.d.). Kenali Maraknya Penipuan Online saat Pandemi - Analisis Data Katadata.

Retrieved November 2, 2020, from https://katadata.co.id/0/analisisdata/5f7c5da0cc927/kenali-maraknya-penipuan-online-saat-pandemi

Schneider, G. P. (2011). *Schneider, Gary P. Electronic Commerce. 9th ed. Boston : Course Technology*.

Setiawan, B. (2017). *Teknik Hitung Manual Analisis Regresi Linear Berganda Dua Variabel Bebas*. 0–9. https://doi.org/10.31227/osf.io/gd73a

Siapa Aplikasi E-wallet dengan Pengguna Terbanyak di Indonesia? (n.d.). Retrieved October 22, 2020, from https://iprice.co.id/trend/insights/e-wallet-terbaik-di-indonesia/

Siponen, M. T. (2000). Conceptual foundation for organizational information security awareness. *Information Management and Computer Security*. https://doi.org/10.1108/09685220010371394

Situmorang, A. P. (n.d.). BPS: Transaksi Belanja Online Masih Didominasi Penduduk di Jawa - Bisnis Liputan6.com. Retrieved January 12, 2021, from 2019 website: https://www.liputan6.com/bisnis/read/4066907/bps-transaksi-belanja-online-masih-didominasi-penduduk-di-jawa

Siyoto, S., & Sodik, A. (2015). Dasar Metodologi Penelitian. *Literasi Media Publishing*, 1–124. Retrieved from https://zenodo.org/record/1117422/files/DASAR METODOLOGI PENELITIAN.pdf

Slezak, P. (2014). Microsoft Excel add-in for the statistical analysis of contingency tables. *Int J Innovation Educ Res*, *2*, 90–100.

Suliyanto. (2018). Pelatihan Metode Pelatihan Kuantitatif. *Journal of Chemical Information and Modeling*, *5*(2), 223–232. https://doi.org/10.1017/CBO9781107415324.004

Urs, B.-A. (2015). Security Issues and Solutions in E-Payment Systems. *Fiat Iustitia*, 21–28.

Vernazi, J. (2011). Getting Started with RStudio. In *Journal of Chemical Information and Modeling*.

Vrîncianu, M., & Popa, L. A. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests. *The AMFITEATRU ECONOMIC Journal*, *12*(28), 388–403.

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. *Learning*, 269, 289.

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program*. https://doi.org/10.6028/NIST.SP.800-50

LAMPIRAN

Kuesioner Penelitian

Survei Analisis Kesadaran Keamanan dalam Penggunaan E-Wallet di Indonesia

Assalamu'alaikum wr.wb,

Bapak/Ibu/Saudara/Saudari yang saya hormati,

Perkenalkan, saya Muhammad Sulthon Alif, mahasiswa tingkat akhir di Jurusan Informatika, Universitas Islam Indonesia, Yogyakarta. Saat ini, saya sedang melakukan penelitian tentang kesadaran keamanan penggunaan e-wallet sebagai Tugas Akhir untuk memenuhi persyaratan memperoleh gelar Sarjana Komputer di Universitas Islam Indonesia.

Semua data yang Bapak/Ibu/Saudara/Saudari isikan akan saya jaga kerahasiaannya dan hanya digunakan untuk kepentingan penelitian semata. Partisipasi dalam penelitian ini bersifat sukarela. Silakan berhenti mengisi jika Bapak/Ibu/Saudara/Saudari berubah pikiran.

Sepuluh (10) responden terpilih akan mendapatkan hadiah pulsa/uang digital sebesar masing-masing Rp. 50.000,-

Atas kesediaan Bapak/Ibu/Saudara/Saudari untuk mengisi survei ini saya ucapkan terima kasih.
* Required

1. Saya bersedia mengisi kuesioner ini secara sukarela tanpa paksaan apapun. *

   Mark only one oval.

   ◯ Ya

Identitas Responden

2. Jenis Kelamin *

   Mark only one oval.

   ◯ Laki-Laki
   ◯ Perempuan

3. Usia (dalam tahun) *

4. Asal Daerah (Provinsi) *

Mark only one oval.

- Nanggroe Aceh Darussalam
- Sumatera Utara
- Sumatera Barat
- Riau
- Kepulauan Riau
- Jambi
- Bengkulu
- Sumatera Selatan
- Kepulauan Bangka Belitung
- Lampung
- Banten
- Jawa Barat
- DKI Jakarta
- Jawa Tengah
- DI Yogyakarta
- Jawa Timur
- Bali
- Nusa Tenggara Barat
- Nusa Tenggara Timur
- Kalimantan Utara
- Kalimantan Barat
- Kalimantan Tengah
- Kalimantan Selatan
- Kalimantan Timur
- Gorontalo
- Sulawesi Utara
- Sulawesi Barat
- Sulawesi Tengah
- Sulawesi Selatan
- Sulawesi Tenggara

- [ ] Sulawesi Tenggara
- [ ] Maluku Utara
- [ ] Maluku
- [ ] Papua Barat
- [ ] Papua

5. Asal Daerah *

Mark only one oval.

- [ ] Kabupaten
- [ ] Kota

6. Nama Kabupaten/Kota *

_____

7. Pendidikan Terakhir *

Mark only one oval.

- [ ] Tidak Tamat SD/sederajat
- [ ] Tamat SD/sederajat
- [ ] Tamat SMP/sederajat
- [ ] Tamat SMA/sederajat
- [ ] Tamat Diploma
- [ ] Tamat Sarjana
- [ ] Tamat Pascasarjana

8. Bidang Pekerjaan *

Mark only one oval.

- ◯ Pelajar/Mahasiswa
- ◯ Pemerintahan dan Administrasi Publik (ASN)
- ◯ Pendidikan
- ◯ Perbankan dan Jasa Keuangan Lainnya
- ◯ Teknologi Informasi & Komunikasi
- ◯ Wiraswasta
- ◯ Tidak Bekerja
- ◯ Lainnya

9. Penghasilan Bulanan *

Mark only one oval.

- ◯ Kurang dari Rp. 1.000.000
- ◯ Rp. 1.000.000 - Rp. 2.999.999
- ◯ Rp. 3.000.000 - Rp. 4.999.999
- ◯ Rp. 5.000.000 - Rp. 9.999.999
- ◯ Rp. 10.000.000 - Rp. 14.999.999
- ◯ Rp. 15.000.000 - Rp. 19.999.999
- ◯ Rp. 20.000.000 - Rp. 34.999.999
- ◯ Rp. 35.000.000 - Rp. 49.999.999
- ◯ Rp. 50.000.000 atau lebih

10. Pilihan Untuk Hadiah yang Diinginkan (bila berkenan)

Mark only one oval.

- ◯ Pulsa
- ◯ OVO
- ◯ Gopay

11. Nomor HP Untuk Hadiah (bila berkenan)

_____

Penggunaan E-Wallet

12. Dari daftar E-Wallet berikut, mana saja yang Anda gunakan? (bisa pilih lebih dari satu) *

Check all that apply.

- ☐ GoPay
- ☐ OVO
- ☐ Dana
- ☐ LinkAja
- ☐ ShopeePay

Other: ☐ _____

13. Dari daftar E-Wallet berikut, mana yang paling sering Anda gunakan? *

Mark only one oval.

- ◯ GoPay
- ◯ OVO
- ◯ Dana
- ◯ LinkAja
- ◯ ShopeePay
- ◯ Other: _____

14. Berapa kali biasanya Anda menggunakan layanan E-Wallet dalam seminggu? *

Mark only one oval.

- ◯ Kurang dari 3 kali
- ◯ 3 sampai 6 kali
- ◯ 7 kali atau lebih

Bagian 1

15. Untuk masing-masing butir pernyataan berikut ini, silakan pilih jawaban yang sesuai dengan apa yang Anda ketahui. *

Mark only one oval per row.

	Benar	Salah	Tidak Tahu
Penggunaan lockscreen di smartphone, baik itu password, pin, pola, atau biometrik adalah suatu keharusan.	◯	◯	◯
Penggunaan password atau pin yang sama untuk beberapa akun berbeda adalah sesuatu yang perlu dihindari.	◯	◯	◯
Penggunaan aplikasi e-wallet saat terhubung ke jaringan Wi-Fi publik sebaiknya dihindari.	◯	◯	◯
Password/PIN e-wallet tidak boleh dibagikan kepada orang lain.	◯	◯	◯
Letakkan dan simpan smartphone hanya di tempat yang aman.	◯	◯	◯
Menyimpan password/PIN dalam bentuk catatan berupa teks adalah sesuatu yang perlu dihindari.	◯	◯	◯
Kode OTP adalah sesuatu yang tidak boleh dibagikan kepada siapa pun.	◯	◯	◯
Instalasi aplikasi dari luar Google Play Store (Android) atau Apple App Store (iOS) adalah sesuatu yang perlu dihindari.	◯	◯	◯
Melakukan update sistem operasi di smartphone secara berkala adalah sesuatu yang sebaiknya dilakukan.	◯	◯	◯
Membiarkan orang lain menggunakan smartphone tanpa pengawasan si pemilik adalah sesuatu yang harus dihindari.	◯	◯	◯
Meninggalkan smartphone tanpa pengawasan langsung adalah sesuatu yang sebaiknya dihindari.	◯	◯	◯
Memastikan aplikasi e-wallet menggunakan	◯	◯	◯

versi terbaru adalah sesuatu yang sebaiknya dilakukan.			
Penggunaan password/PIN yang mudah ditebak seperti nama sendiri, tanggal lahir, angka berurutan, atau angka berulang adalah sesuatu yang perlu dihindari.			

Bagian 2

16. Silakan pilih jawaban yang paling sesuai dengan kondisi Anda untuk masing-masing butir pernyataan berikut ini. *

Mark only one oval per row.

	Benar	Salah	Tidak Tahu
Saya sadar untuk menggunakan lockscreen di smartphone, baik itu password, pin, pola, atau biometrik agar lebih aman.	◯	◯	◯
Saya sadar untuk menggunakan password atau pin yang berbeda untuk beberapa akun yang digunakan.	◯	◯	◯
Saya sadar untuk menggunakan e-wallet hanya melalui data seluler dari sim card sendiri.	◯	◯	◯
Saya sadar untuk menyimpan password/PIN e-wallet hanya untuk diri sendiri.	◯	◯	◯
Saya sadar untuk meletakkan dan menyimpan smartphone hanya di tempat yang aman.	◯	◯	◯
Saya sadar untuk menghindari password/PIN e-wallet yang disimpan dalam bentuk catatan berupa teks.	◯	◯	◯
Saya sadar untuk menyimpan kode OTP hanya untuk diri sendiri.	◯	◯	◯
Saya sadar untuk menginstall aplikasi hanya dari Google Play Store (Android) atau Apple App Store (iOS).	◯	◯	◯
Saya sadar untuk melakukan update sistem operasi di smartphone secara berkala.	◯	◯	◯
Saya sadar untuk mengawasi smartphone milik sendiri ketika sedang digunakan oleh orang lain.	◯	◯	◯
Saya sadar untuk meninggalkan smartphone di tempat yang bisa diawasi langsung oleh diri sendiri.	◯	◯	◯

Saya sadar untuk memastikan aplikasi e-wallet menggunakan versi terbaru ketika hendak melakukan transaksi/pembayaran.			
Saya sadar untuk menggunakan password /PIN yang kompleks agar tidak mudah ditebak.			

Bagian 3

17. Silakan pilih jawaban yang paling sesuai dengan kebiasaan Anda untuk masing-masing butir pernyataan berikut ini. *

Mark only one oval per row.

	Benar	Salah
Saya terbiasa melakukan pengamanan menggunakan lockscreen di smartphone, baik itu password, pin, pola, atau biometrik.	◯	◯
Saya terbiasa untuk tidak menggunakan password atau pin yang sama untuk beberapa akun berbeda.	◯	◯
Saya terbiasa untuk tidak menggunakan e-wallet ketika terhubung ke jaringan Wi-Fi publik.	◯	◯
Saya terbiasa untuk tidak membagikan password/PIN e-wallet kepada orang lain.	◯	◯
Saya terbiasa untuk tidak meletakkan dan menyimpan smartphone di tempat sembarangan.	◯	◯
Saya terbiasa untuk tidak menyimpan password/PIN dalam bentuk catatan berupa teks.	◯	◯
Saya terbiasa untuk tidak membagikan kode OTP kepada siapapun.	◯	◯
Saya terbiasa melakukan instalasi aplikasi hanya dari Google Play Store (Android) atau Apple App Store (iOS).	◯	◯
Saya terbiasa melakukan update sistem operasi di smartphone secara berkala.	◯	◯
Saya terbiasa untuk tidak membiarkan orang lain menggunakan smartphone milik saya tanpa pengawasan.	◯	◯
Saya terbiasa untuk tidak meninggalkan smartphone tanpa pengawasan langsung.	◯	◯
Saya terbiasa melakukan pengecekan versi	◯	◯

terbaru aplikasi e-wallet yang hendak digunakan.		
Saya terbiasa untuk tidak menggunakan password/PIN yang mudah ditebak seperti nama sendiri, tanggal lahir, angka berurutan, atau angka berulang.		

Terima Kasih

Terima kasih atas partisipasi Anda.