

**ANALISIS TINGKAT KESADARAN KEAMANAN SIBER
PADA PENGGUNA AKTIF DAERAH ISTIMEWA
YOGYAKARTA (DIY)**



Disusun Oleh:

N a m a : Arya Nanda M.P.
NIM : 19523188

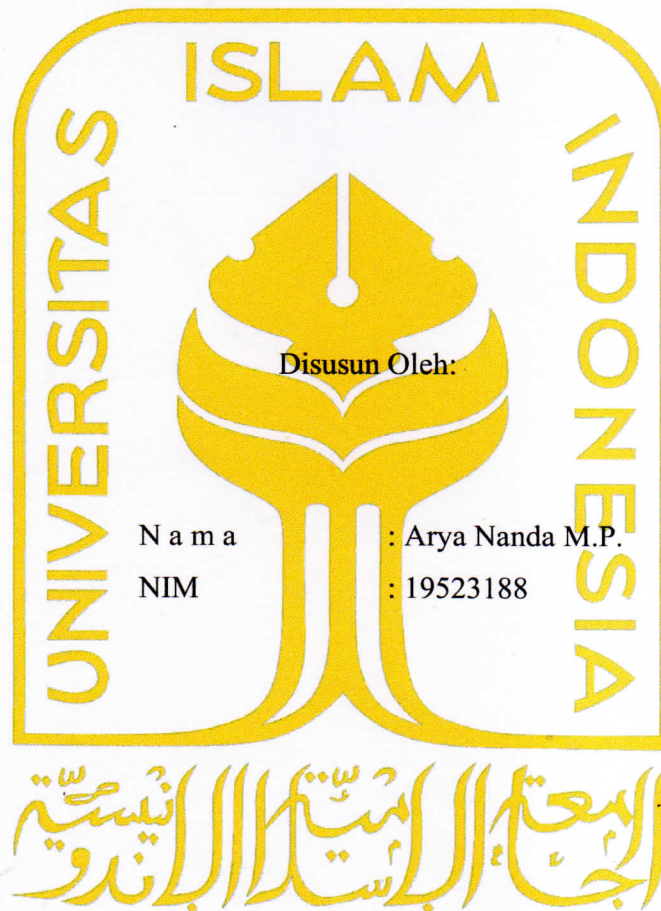
**PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA**

2024

HALAMAN PENGESAHAN DOSEN PEMBIMBING

**ANALISIS TINGKAT KESADARAN KEAMANAN SIBER
PADA PENGGUNA AKTIF DAERAH ISTIMEWA
YOGYAKARTA (DIY)**

TUGAS AKHIR



Yogyakarta, 01 Juni 2024

Pembimbing 1,

Signer ID: DLUSVECN14...

(Fayruz Rahma, S.T., M.Eng.)

Pembimbing 2,

(Elyza Gustri Wahyuni, S.T., M.Cs.)

HALAMAN PENGESAHAN DOSEN PENGUJI

ANALISIS TINGKAT KESADARAN KEAMANAN SIBER PADA PENGGUNA AKTIF DAERAH ISTIMEWA YOGYAKARTA (DIY)

TUGAS AKHIR

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

Yogyakarta, 16 January 2025

Tim Penguji

Elyza Gustri Wahyuni, S.T., M.Cs.

Anggota 1

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

Anggota 2

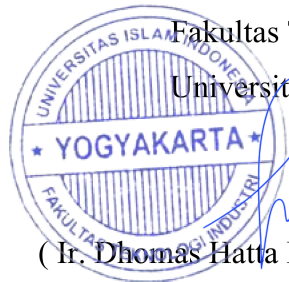
Sri Mulyati, S.Kom., M.Kom.

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia



(Ir. Thomas Hatta Fudholi, S.T., M.Eng., Ph.D)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama : Arya Nanda Mahardika Putra

NIM : 19523188

Tugas akhir dengan judul:

ANALISIS TINGKAT KESADARAN KEAMANAN SIBER PADA PENGGUNA AKTIF DAERAH ISTIMEWA YOGYAKARTA (DIY)

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian 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 risiko dan konsekuensi apapun.

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

Yogyakarta, 16 January 2025



(Arya Nanda Mahardika Putra)

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 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 perkuliahan di kampus dengan canda tawa dan hiburan mereka yang sangat mengasyikkan.

HALAMAN MOTO

وَلَا تَهِنُوا وَلَا تَحْزَنُوا وَأَنْتُمْ الْأَعْلَوْنَ إِنْ كُنْتُمْ مُؤْمِنِينَ

"Jangan kamu merasa lemah dan jangan bersedih, sebab kamu paling tinggi derajatnya jika kamu beriman." (Q.S Ali Imran: 139)

“Unless you stop trying, how can you not fail anymore.”
– Felix Arvid Ulf Kjellberg

فَإِنْ لَّمْ يَسْتَجِيبُوا لَكَ فَاعْلَمْ أَنَّهَا هَوَاءٌ هُمْ وَمَنْ أَضَلُّ
مِمَّنِ اتَّبَعَ هَوَاهُ بِغَيْرِ هُدًى مِّنَ اللَّهِ إِنَّ اللَّهَ لَا يَهْدِي الْقَوْمَ الظَّالِمِينَ

"Dan siapakah yang lebih sesat daripada orang yang mengikuti hawa nafsunya dengan tidak mendapat petunjuk dari Allah sedikit pun. Sesungguhnya Allah tidak memberi petunjuk kepada orang-orang yang zalim." (Q.S Al-Qashas: 50)

KATA PENGANTAR

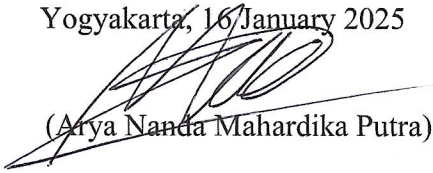
Puji syukur atas kehadiran Allah SWT, karena atas berkat rahmat dan karunia-Nya saya dapat menyelesaikan tugas akhir yang berjudul “Analisis Kesadaran Keamanan dalam Penggunaan *E-wallet* di Indonesia”. Sholawat dan salam dicurahkan kepada Muhammad SAW, yang telah menjadi sosok inspirasi suri tauladan 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. Kedua kakak tersayang yang telah memberi ide dan semangat dalam penulisan tugas akhir ini.
3. Bapak Irving Vitra Paputungan, S.T., M.Sc., Ph.D selaku Ketua Program Studi Informatika
4. Ibu Fayruz Rahma, S.T., M.Eng dan Ibu Elyza Gustri Wahyuni, S.T., M.Cs.. 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.
5. Ibu Aridhanyati Arifin, S.T., M.Cs. selaku dosen pembimbing akademik yang membantu selama masa perkuliahan saya.
6. Seluruh dosen Program Studi Informatika yang banyak memberikan ilmu, pelajaran, pengalaman, serta nasihat selama saya berkuliah.
7. 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, 16 January 2025


(Arya Nanda Mahardika Putra)

SARI

Peningkatan penggunaan E-wallet di Daerah Istimewa Yogyakarta terlihat jelas dalam beberapa tahun terakhir. Meskipun banyak kemudahan dan kepraktisan yang ditawarkan, ada pula berbagai risiko keamanan yang mengancam pengguna. Mengingat bahwa faktor manusia memainkan peran penting dalam dunia siber dan informasi, kesadaran tentang keamanan menjadi sangat krusial. Dengan menggunakan data primer dari survei online yang melibatkan 328 pengguna E-wallet di daerah tersebut, studi ini bertujuan untuk mengukur tingkat kesadaran keamanan siber dalam penggunaan E-wallet serta menganalisis seberapa banyak pengetahuan yang dimiliki pengguna, dampaknya terhadap kebiasaan, dan perbedaan tingkat kesadaran berdasarkan faktor demografis seperti usia, lokasi (kabupaten/kota), pendidikan terakhir, dan pendapatan bulanan. Menurut pengukuran menggunakan model analisis regresi linear berganda, tingkat kesadaran keamanan pengguna E-wallet di Daerah Istimewa Yogyakarta secara umum dapat dikatakan cukup baik dengan skor rata-rata keseluruhan sebesar 78%. Namun, masih terdapat peluang untuk meningkatkan pengetahuan, sikap, dan perilaku pengguna, terutama dalam hal keamanan PIN/Password yang memiliki skor 85%, penggunaan perangkat lunak sebesar 79%, dan pemahaman tentang keamanan internet yang masih berada di angka 71%, yang lebih rendah dibandingkan dengan kesadaran terhadap perangkat keras yang mencapai 77%. Analisis juga menunjukkan bahwa pendapatan dan pendidikan merupakan dua faktor utama yang memengaruhi tingkat kesadaran keamanan siber. Responden dengan tingkat pendidikan yang lebih tinggi, cenderung memiliki kesadaran lebih baik, dimana Diploma yang berada di angka 81%. Sementara itu, faktor pendapatan menunjukkan bahwa kelompok dengan penghasilan Rp3.000.000 - Rp4.999.999 memiliki tingkat kesadaran tertinggi sebesar 79%, sedangkan kelompok dengan penghasilan di atas Rp10.000.000 memiliki skor kesadaran yang lebih rendah, yaitu 73%. Selain itu, faktor domisili juga berkontribusi pada perbedaan tingkat kesadaran keamanan siber, di mana Kabupaten Sleman memiliki tingkat kesadaran tertinggi sebesar 79%, sedangkan Kabupaten Kulon Progo menunjukkan tingkat kesadaran terendah dengan skor 74%. Temuan dari penelitian ini dapat digunakan untuk merancang berbagai intervensi atau kebijakan guna meningkatkan kesadaran keamanan di kalangan seluruh pengguna E-wallet di Daerah Istimewa Yogyakarta.

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

GLOSARIUM

<i>E-wallet</i>	dompet digital yang digunakan untuk melakukan pembayaran transaksi jual beli secara non tunai.
E-Commerce	proses pembelian dan penjualan sebuah produk yang dilakukan secara elektronik.
Malware	perangkat lunak berbahaya yang dirancang untuk merusak, mencuri, atau mengeksploitasi perangkat, server, atau jaringan yang dapat diprogram
Non-probability Sampling	merupakan pengambilan sampel yang tidak memberikan peluang yang sama kepada anggota populasi, dan penentuannya tidaklah acak.
Purposive Sampling	metodologi pengambilan sampel secara acak dimana kelompok sampel ditargetkan memiliki atribut-atribut tertentu
Phishing	kejahatan siber yang dilakukan untuk mendapatkan informasi pribadi pengguna secara tidak sah.
Ransomware	jenis virus atau malware berbahaya yang digunakan untuk mengenkripsi data pengguna pada suatu perangkat komputer atau jaringan.
Worm	malware yang bisa menggandakan diri lalu menyebarkannya ke dalam semua jaringan tanpa adanya campur tangan dari pengguna.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN DOSEN PEMBIMBING	ii
HALAMAN PENGESAHAN DOSEN PENGUJI	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR.....	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTO	vi
KATA PENGANTAR.....	vii
SARI.....	viii
GLOSARIUM	ix
DAFTAR ISI	x
DAFTAR TABEL	xii
DAFTAR GAMBAR.....	xiii
BAB I PENDAHULUAN	14
1.1 Latar Belakang	14
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
BAB II TINJAUAN PUSTAKA	5
2.1 Landasan Teori.....	5
2.1.1 <i>E-Wallet</i>	5
2.1.2 Konsep <i>Cyber security</i>	6
2.1.3 Ancaman dan Risiko dalam <i>Cyber security</i>	6
2.1.4 Kesadaran Keamanan Siber (<i>Cyber security Awareness Theory</i>)	8
2.1.5 <i>Knowledge Attitude and Behavior</i>	9
2.1.6 HAIS-Q (<i>Human Aspects of Information Security Questionnaire</i>)	10
2.1.7 Analisis Regresi Linear Berganda.....	11
2.1.8 Skala Likert.....	12
2.1.9 Analisis Deskriptif	13
2.2 Penelitian Sebelumnya	13
BAB III METODOLOGI PENELITIAN	16
3.1 Studi Literatur	17
3.2 Metode Penelitian	17
3.3 Teknik Pengumpulan Data.....	17
3.4 Jenis dan Sumber Data	18
3.5 Populasi dan Sampel	18
3.6 Operasional Variabel.....	19
3.6.1 Variabel Dependen.....	20
3.6.2 Variabel Independen	21
3.7 Analisis Deskriptif	22
3.8 Analisis Regresi Linear Berganda.....	22
3.9 Kesimpulan dan Rekomendasi	22
BAB IV HASIL DAN PEMBAHASAN.....	23
4.1 Hasil Analisis Deskriptif.....	23
4.1.1 Usia Responden.....	25
4.1.2 Domisili Responden.....	26

4.1.3	Pendidikan Terakhir	26
4.1.4	Pekerjaan Responden	27
4.1.5	Penghasilan Responden.....	28
4.2	Karakteristik Penggunaan <i>E-wallet</i>	28
4.2.1	Jenis <i>E-wallet</i> yang Sering Digunakan Responden.....	29
4.2.2	Frekuensi Penggunaan <i>E-wallet</i> Tertinggi.....	30
4.2.3	Sumber Informasi Keamanan Siber Responden	30
4.3	Hasil Skor Kesadaran Keamanan Siber	31
4.3.1	Skor Kesadaran Keamanan Siber berdasarkan Usia	35
4.3.2	Skor Kesadaran Keamanan Siber berdasarkan Domisili	36
4.3.3	Skor Kesadaran Keamanan Siber berdasarkan Pendidikan Terakhir.....	37
4.3.4	Skor Kesadaran Keamanan Siber Berdasarkan Pekerjaan.....	40
4.3.5	Skor Kesadaran Keamanan Siber Berdasarkan Penghasilan	42
4.4	Hasil Analisis Regresi Berganda.....	43
	BAB V.....	46
	KESIMPULAN DAN SARAN.....	46
5.1	Kesimpulan	46
5.2	Saran.....	47
	DAFTAR PUSTAKA.....	48
	LAMPIRAN	51

DAFTAR TABEL

Tabel 2.1 Skala Likert.....	13
Tabel 2.2 Penelitian Terdahulu.....	14
Tabel 4.1 Hasil Analisis Deskriptif.....	24
Tabel 4.2 Persentase Karakteristik Penggunaan <i>E-wallet</i>	30
Tabel 4.3 Kriteria Kesadaran Keamanan	32
Tabel 4.4 Tingkat Kesadaran Keamanan Siber.....	33
Tabel 4.5 Skor Kesadaran Keamanan Siber berdasarkan Usia.....	34
Tabel 4.6 Skor Kesadaran Keamanan Siber berdasarkan Domisili	36
Tabel 4.7 Skor Kesadaran Keamanan Siber berdasarkan Pendidikan Terakhir	37
Tabel 4.8 Skor Kesadaran Keamanan Siber berdasarkan Pekerjaan	39
Tabel 4.9 Skor Kesadaran Keamanan Siber berdasarkan Penghasilan.....	41
Tabel 4.10 Hasil Olah Data Regresi Linear Variabel Usia.....	42
Tabel 4.11 Hasil Olah Data Regresi Linear Variabel Domisili	44
Tabel 4.12 Hasil Olah Data Regresi Linear Variabel Pendidikan Terakhir	44
Tabel 4.13 Hasil Olah Data Regresi Linear Variabel Pekerjaan	44
Tabel 4.14 Hasil Olah Data Regresi Linear Variabel Penghasilan.....	44
Tabel 1 Lampiran.....	50

DAFTAR GAMBAR

Gambar 3.1 Diagram Alur Penelitian	16
Gambar 4.1 Histogram Usia Responden.....	26
Gambar 4.2 Diagram <i>Pie</i> Domisili Responden.....	27
Gambar 4.3 Diagram <i>Pie</i> Pendidikan Terakhir Responden.....	28
Gambar 4.4 Diagram <i>Pie</i> Pekerjaan Responden.....	28
Gambar 4.5 <i>Diagram Pie</i> Penghasilan Responden.....	39
Gambar 4.6 <i>Diagram Pie</i> Jenis <i>E-wallet</i> Responden.....	30
Gambar 4.7 <i>Diagram Pie</i> Frekuensi Penggunaan <i>E-wallet</i>	31
Gambar 4.8 <i>Diagram Pie</i> Sumber Informasi Keamanan Siber Responden.....	32

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, penggunaan teknologi informasi dan komunikasi telah menjadi bagian integral dari kehidupan sehari-hari masyarakat. Seiring waktu, perkembangan teknologi memudahkan pengguna dalam melakukan pembelian dengan mengubah sistem pembayaran dari tunai menjadi nontunai. Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam hal transaksi keuangan. Salah satu inovasi yang semakin populer adalah penggunaan dompet elektronik atau (Rahmawati & Yuliana, 2020). menawarkan kemudahan dan kecepatan dalam melakukan transaksi tanpa perlu membawa uang tunai, yang sangat mendukung gaya hidup digital masyarakat modern. Sebagian besar pengguna memanfaatkan aplikasi untuk berbagai keperluan, seperti pemesanan makanan secara *online*, layanan transportasi *online*, dan belanja *online* (Anjani, Awali, & Misidawati, 2022).

Masuknya teknologi telah memengaruhi berbagai aspek kehidupan manusia, termasuk dalam jual beli dan penggunaan uang tunai. Di Indonesia, banyak layanan keuangan berbasis digital bermunculan, termasuk . Layanan ini memungkinkan pengguna melakukan transaksi untuk berbagai keperluan dengan saldo yang tersimpan di . Di kota-kota besar, terutama Daerah Istimewa Yogyakarta DIY, layanan ini banyak digunakan oleh orang-orang dalam usia produktif (Muhammad, 2022). Daerah Istimewa Yogyakarta DIY dikenal sebagai salah satu pusat pendidikan dan teknologi di Indonesia, dengan populasi yang didominasi oleh generasi muda yang adaptif terhadap inovasi digital. Banyaknya pengguna aktif di wilayah ini mencerminkan pertumbuhan transaksi nontunai, yang membawa risiko keamanan siber yang signifikan (Muhammad, 2022). Tingginya penetrasi teknologi di kalangan masyarakat Daerah Istimewa Yogyakarta DIY menjadi alasan kuat untuk mengeksplorasi sejauh mana kesadaran keamanan siber mereka dalam penggunaan .

Alasan utama penggunaan adalah kepraktisannya, karena pengguna tidak perlu menyiapkan uang tunai saat bertransaksi. Bagi penjual, mereka tidak perlu repot menyediakan uang kembalian karena pembayaran dilakukan dengan nominal yang tepat. Beberapa layanan di Indonesia hadir dalam bentuk *mobile wallet* atau aplikasi (Aaputra, Didi Rosiyadi, Windu Gata, & Syepri Maulana Husain, 2019).

Meskipun efisien dan praktis, penelitian oleh Susanti dan Dwiana Putra (2023) menunjukkan bahwa banyak generasi milenial masih menggunakan uang tunai untuk membayar barang dan jasa (Susanti & Dwiana Putra, 2023). Hal ini disebabkan oleh kurangnya pemahaman tentang manfaat dan kemudahan sehingga kepercayaan terhadap pembayaran belum sejalan dengan tujuan utamanya yang menyatakan bahwa transaksi memudahkan dan memberikan keamanan bagi pengguna.

Keamanan siber (*cyber security*) menjadi isu penting mengingat tingginya ancaman terhadap data pribadi dan finansial pengguna. Keamanan siber juga dapat diartikan sebagai upaya untuk menahan serangan-serangan di dunia siber (Faliandy, M Yonandio Lazuardi, & Tata Sutabri, 2023). Kejahatan siber seperti pencurian identitas, *phishing*, dan *malware* dapat merugikan pengguna secara finansial maupun psikologis. Oleh karena itu, kesadaran akan pentingnya keamanan siber dalam penggunaan menjadi faktor krusial yang harus ditingkatkan.

Penelitian oleh Harminingtyas, dkk. (2020) mendukung penelitian ini dengan menunjukkan bahwa persepsi manfaat, kemudahan, dan keamanan secara positif dan signifikan memengaruhi penggunaan di Kota Semarang. Persepsi keamanan memiliki pengaruh dominan terhadap keputusan penggunaan, menegaskan bahwa keamanan adalah faktor terpenting karena pengguna merasa aman dan terlindungi.

Namun, tingkat kesadaran keamanan siber di kalangan pengguna aktif masih bervariasi dan dipengaruhi oleh berbagai faktor. Tingkat pengetahuan pengguna tentang ancaman keamanan siber dan cara melindungi diri menjadi faktor utama (Alif & Pratama, 2021). Edukasi yang baik tentang praktik keamanan siber dapat meningkatkan kesadaran dan kewaspadaan pengguna. Selain itu, pengalaman sebelumnya dengan insiden keamanan siber atau kejahatan digital juga dapat memengaruhi tingkat kesadaran dan kewaspadaan pengguna. Keberadaan fitur keamanan seperti autentikasi dua faktor, enkripsi data, dan notifikasi transaksi dapat meningkatkan rasa aman pengguna. Inisiatif dari pemerintah, penyedia layanan, dan komunitas untuk meningkatkan kesadaran melalui kampanye dan program edukasi memainkan peran penting dalam membentuk persepsi dan perilaku pengguna (Faliandy et al., 2023). Faktor-faktor demografis seperti usia, tingkat pendidikan, dan latar belakang pekerjaan juga memengaruhi tingkat kesadaran keamanan siber, dengan pengguna yang lebih muda dan lebih terdidik cenderung lebih sadar akan isu keamanan siber (Muhammad, 2022).

Berdasarkan masalah yang ada, penelitian ini bertujuan untuk mengeksplorasi tingkat kesadaran keamanan siber di kalangan pengguna aktif. Metode yang digunakan dalam penelitian ini adalah metode deskriptif dengan pendekatan kuantitatif. Metode ini menjelaskan

pengaruh pengetahuan keamanan siber pada platform serta faktor terhadap kesadaran keamanan siber di pengguna aktif Provinsi Daerah Istimewa Yogyakarta DIY. Analisis data yang digunakan dalam penelitian ini adalah deskriptif dan analisis regresi linear berganda untuk menguji faktor-faktor yang dapat memengaruhi tingkat kesadaran keamanan siber pada pengguna aktif. Dengan memahami sejauh mana pengguna menyadari dan mengaplikasikan praktik keamanan yang baik, peneliti dapat mengidentifikasi celah-celah yang ada dan merumuskan strategi edukasi yang lebih efektif. Hal ini diharapkan dapat meminimalisir risiko keamanan dan meningkatkan kepercayaan masyarakat terhadap penggunaan. Kajian ini menjadi penting mengingat tren penggunaan yang terus meningkat, terutama di masa sekarang di mana transaksi digital menjadi pilihan utama untuk mengurangi kontak fisik. Penelitian ini diharapkan dapat memberikan kontribusi dalam upaya memperkuat ekosistem digital yang aman dan terpercaya, serta memberikan rekomendasi bagi penyedia layanan dalam meningkatkan sistem keamanan.

1.2 Rumusan Masalah

Dalam penelitian yang berjudul " Analisis Tingkat Kesadaran Keamanan Siber Pada Pengguna Aktif *E-wallet* Daerah Istimewa Yogyakarta (DIY)", rumusan masalah yang akan diangkat adalah sebagai berikut:

1. Bagaimana tingkat kesadaran pengguna aktif terhadap keamanan siber?
2. Faktor-faktor apa saja yang memengaruhi kesadaran keamanan siber di kalangan pengguna aktif ?

1.3 Batasan Masalah

Dalam penelitian yang berjudul "Analisis Tingkat Kesadaran Keamanan Siber Pada Pengguna Aktif *E-wallet* Daerah Istimewa Yogyakarta (DIY)", batasan masalah yang ditetapkan adalah sebagai berikut:

1. Penelitian ini dibatasi pada pengguna aktif di wilayah Daerah Istimewa Yogyakarta DIY.
2. Penelitian ini hanya akan mengkaji aspek-aspek kesadaran keamanan siber, seperti pengetahuan tentang ancaman siber, kesadaran tentang pentingnya keamanan data, dan perilaku pengguna dalam menjaga keamanan.
3. yang diteliti adalah yang memiliki fitur dasar seperti pembayaran, transfer uang, dan penyimpanan data finansial.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada, tujuan dari penelitian ini di antaranya:

1. Untuk menilai sejauh mana pengguna aktif memiliki kesadaran tentang pentingnya keamanan siber dalam penggunaan .
2. Untuk meneliti berbagai faktor yang memengaruhi tingkat kesadaran keamanan siber di kalangan pengguna aktif , seperti tingkat pendidikan, pengetahuan teknologi, dan pengalaman penggunaan .
3. Untuk mengidentifikasi risiko-risiko keamanan yang paling sering dihadapi oleh pengguna aktif , seperti *phishing*, *malware*, dan pencurian identitas, serta menilai tingkat kesadaran pengguna terhadap risiko-risiko tersebut.

BAB II

TINJAUAN PUSTAKA

Penelitian ini bertujuan untuk mengeksplorasi tingkat kesadaran keamanan siber di kalangan pengguna aktif *e-wallet*, dengan harapan dapat memberikan wawasan yang berguna bagi pengguna dan pengembang teknologi finansial. Pada bab ini akan dibahas beberapa teori-teori yang menjadi dasar dari penelitian ini.

2.1 Landasan Teori

Landasan teori adalah kumpulan konsep, definisi, proposisi, dan teori yang digunakan sebagai dasar untuk penelitian dan pengembangan pengetahuan di suatu bidang tertentu. Landasan teori memberikan kerangka konseptual yang membantu peneliti memahami fenomena yang sedang dipelajari dan menentukan metode penelitian yang akan digunakan. Dalam konteks penelitian tentang kesadaran keamanan siber di kalangan pengguna, landasan teori mencakup beberapa aspek penting yang relevan dengan topik ini, di antaranya:

2.1.1 *E-Wallet*

, juga dikenal sebagai dompet digital, semakin populer di kalangan masyarakat yang beralih menggunakannya karena berbagai promo menarik yang ditawarkan. *The Economic Times* menyatakan bahwa dompet digital adalah jenis akun prabayar yang dilindungi kata sandi (Warta Ekonomi, 2019), memungkinkan pengguna untuk menyimpan uang untuk berbagai transaksi *online*, seperti membayar makanan, belanja *online*, dan tiket penerbangan (Kusnawan, Diana, Andy, & Tjong, 2019).

Berdasarkan Peraturan Bank Indonesia Nomor 18/40/PBI/2016, adalah layanan elektronik untuk menyimpan data instrumen pembayaran, seperti alat pembayaran dengan kartu dan uang elektronik, yang dapat menampung dana untuk melakukan pembayaran (Bank Indonesia, 2016). merupakan implementasi perangkat lunak yang memungkinkan pengguna menyimpan uang secara digital, melakukan pembayaran digital, dan berbagai transaksi tanpa uang tunai, tanpa menggunakan media seperti kartu dan hanya melakukan transaksi melalui perangkat seperti komputer atau *smartphone*. Berbeda dengan kartu kredit atau kartu debit, transaksi menggunakan dilakukan secara langsung tanpa melalui pihak ketiga atau perantara (Umiyati, Putri, & Maya, 2021).

2.1.2 Konsep *Cyber security*

Pada dekade kedua abad ke-21, awalan "cyber" telah terintegrasi dengan konsep-konsep seperti "cyberculture", "cybersex", dan "cyberwar", yang semuanya berkaitan dengan media digital, realitas virtual, dan internet. Dalam budaya populer, penggunaan awalan dan imbuhan kata-kata ini seringkali kabur, seperti yang terlihat pada gerakan sastra "cyberpunk". Selain itu, sejak munculnya internet, kata "network" telah menjadi metafora penting yang mendapat perhatian luas di hampir setiap disiplin ilmu kontemporer dan institusi besar. Pada tahun 1948, awalan "cyber" pertama kali digunakan dalam istilah "cybernetics", yang digambarkan sebagai "studi tentang pesan sebagai sarana untuk mengendalikan mesin dan masyarakat" (Chotimah, 2019).

Cyber security, atau keamanan siber, adalah praktik melindungi sistem, jaringan, dan program dari serangan digital yang bertujuan untuk mengakses, mengubah, atau merusak informasi sensitif, memeras uang dari pengguna, atau mengganggu proses bisnis normal (Yuniarti, Alfarizy, Siallagan, & Rizkianfi, 2023). Keamanan siber merupakan kegiatan pencegahan dan perlindungan terhadap sumber daya telematika untuk mencegah terjadinya kejahatan di dunia maya. *Cyber security* juga dapat diartikan sebagai upaya untuk melindungi dari serangan-serangan di dunia siber. Penerapan keamanan siber tidak hanya dilakukan pada perangkat atau program, tetapi juga melibatkan pemberian pemahaman kepada sumber daya manusia tentang pentingnya kesadaran keamanan. Dalam konteks keamanan siber, faktor manusia sangat penting karena peran mereka sebagai pengguna dalam proses keamanan dapat berdampak positif atau negatif terhadap upaya keamanan siber (Faliandy et al., 2023).

2.1.3 Ancaman dan Risiko dalam *Cyber security*

Ancaman keamanan siber adalah tantangan kompleks yang membutuhkan pemahaman mendalam untuk melindungi infrastruktur TI dari ancaman yang terus berkembang. Ancaman ini dapat berasal dari berbagai sumber, baik eksternal maupun internal organisasi. Untuk memberikan pemahaman yang lebih mendetail, ancaman-ancaman tersebut dapat diklasifikasikan ke dalam tiga kategori utama, di antaranya (Hoshmand, Ratnawati, & Korespondensi, 2023):

1. Ancaman Fisik

Ancaman fisik mencakup potensi kerusakan atau kehilangan terhadap komponen fisik infrastruktur TI. Ini melibatkan risiko pencurian perangkat keras, kerusakan fisik, atau sabotase. Ancaman fisik dapat menyebabkan kerusakan pada integritas perangkat keras,

pusat data, atau fasilitas fisik lainnya, dan dampaknya meliputi gangguan operasional, kehilangan data, atau bahkan ketidakberlanjutan layanan. Ancaman fisik terhadap infrastruktur TI merupakan ancaman yang memerlukan langkah-langkah pencegahan dan perlindungan yang teliti. Potensi kerusakan atau kehilangan pada komponen fisik dapat berdampak signifikan terhadap integritas, ketersediaan, dan operasional keseluruhan infrastruktur TI. Oleh karena itu, strategi pencegahan dan perlindungan terhadap ancaman fisik menjadi sangat penting dalam mengurangi risiko yang terkait dengan aspek fisik ini. Pencegahan pencurian perangkat keras adalah salah satu langkah yang krusial karena pencurian perangkat keras dapat menyebabkan kerugian finansial dan kehilangan data yang penting.

2. Ancaman Logikal

Ancaman logis terhadap infrastruktur TI melibatkan serangkaian serangan yang ditujukan pada aspek digital. Mengenali dan menangani ancaman logis ini memerlukan strategi yang menyeluruh, termasuk deteksi dini, pencegahan, dan tanggapan cepat untuk mengurangi potensi dampak yang mungkin timbul. Istilah umum "*malware*" mencakup berbagai jenis perangkat lunak berbahaya, seperti virus, *worm*, dan *trojan*. Serangan *malware* bertujuan untuk menyusup ke dalam sistem komputer dan merusaknya. Virus dapat menempel pada *file* atau program dan menyebar saat *file* atau program tersebut dijalankan. *Worm* dapat menyebar sendiri melalui jaringan, sementara *trojan* menyamar sebagai program berguna untuk menipu pengguna dan kemudian mengeksploitasi sistem. Selain merusak sistem, *malware* juga dapat mencuri data sensitif seperti informasi *login* atau keuangan.

Pendekatan yang menyeluruh diperlukan dalam menghadapi ancaman logis terhadap infrastruktur TI, yang mencakup pencegahan, deteksi dini, dan respons yang cepat. Dengan menggabungkan teknologi keamanan, pelatihan untuk pengguna, dan sistem pemantauan yang efektif, organisasi dapat mengurangi risiko dari serangan logis, melindungi integritas sistem, dan meminimalkan potensi kerugian data. Terus meningkatkan strategi keamanan sesuai dengan perkembangan teknologi dan taktik serangan siber yang baru akan menjadi kunci dalam menjaga keamanan infrastruktur TI.

3. Ancaman Operasional

Ancaman operasional adalah tantangan serius yang muncul dari faktor internal di dalam sebuah organisasi, yang dapat berupa kesalahan manusia, kelalaian, atau pelanggaran terhadap prosedur keamanan. Kesalahan manusia seperti konfigurasi sistem

yang salah atau penghapusan data secara tidak sengaja dapat mengganggu kelangsungan operasional. Untuk mengatasi hal ini, pelatihan karyawan secara rutin dan otomatisasi proses dapat menjadi langkah pencegahan yang efektif. Kelalaian, yang mencakup kurangnya perhatian dalam tugas-tugas operasional, juga dapat menjadi sumber ancaman. Kebijakan keamanan yang jelas dan pemantauan aktivitas pengguna membantu mengurangi risiko dari kelalaian ini. Ancaman juga dapat timbul dari ketidakpatuhan terhadap prosedur keamanan yang telah ditetapkan.

Ancaman dan Risiko dalam Keamanan Siber menurut penelitian (Arfan Dwi Madya, Bagas Djoko Haryanto, & Devi Putri Ningsih, 2023) di antaranya:

1. *Malware*: Ini adalah perangkat lunak berbahaya yang diciptakan untuk merusak, mengganggu, atau memperoleh akses tidak sah ke sistem komputer. *Malware* bisa berupa virus, *worm*, *trojan*, *spyware*, atau *ransomware*. Mereka dapat menyebabkan kerusakan pada sistem, mencuri informasi sensitif, atau menghambat kinerja perangkat.
2. *Phishing*: Ini adalah taktik yang digunakan oleh penipu untuk memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik. Penyerang sering menggunakan email, pesan teks, atau situs *web* palsu untuk memancing korban agar memberikan informasi pribadi mereka.
3. *Ransomware*: Jenis *malware* ini mengenkripsi atau mengunci data korban dan kemudian mengancam untuk mempublikasikan atau menghancurkan data tersebut kecuali tebusan dibayar. Korban sering kali diminta untuk membayar tebusan dalam bentuk mata uang kripto untuk mendapatkan kunci dekripsi dan mengembalikan akses ke data mereka.
4. Serangan *Man-in-the-Middle* (MitM): Ini adalah serangan di mana penyerang menyadap komunikasi antara dua pihak yang berinteraksi secara langsung. Dalam skenario ini, penyerang dapat memata-matai atau bahkan mengubah pesan yang dikirim antara kedua pihak tanpa sepengetahuan mereka. Hal ini dapat digunakan untuk mencuri informasi sensitif atau mengarahkan transaksi ke situs palsu.

2.1.4 Kesadaran Keamanan Siber (*Cyber security Awareness Theory*)

Teori Kesadaran Keamanan Siber (*Cyber security Awareness Theory*) mengacu pada pemahaman individu tentang potensi ancaman siber dan tindakan yang dapat diambil untuk melindungi diri dari ancaman tersebut. Teori ini menjelaskan bagaimana tingkat kesadaran

individu terhadap risiko keamanan siber dapat memengaruhi perilaku mereka dalam menggunakan teknologi digital, termasuk (Wathoni et al., 2023).

Dalam konteks , individu yang memiliki tingkat kesadaran keamanan siber yang tinggi cenderung lebih waspada terhadap potensi risiko seperti pencurian identitas, serangan *malware*, atau kebocoran informasi keuangan saat menggunakan layanan . Mereka mungkin lebih cenderung untuk mengadopsi praktik keamanan seperti penggunaan sandi yang kuat, mengaktifkan fitur keamanan tambahan, dan menghindari tautan atau situs web yang mencurigakan. Teori ini juga menyoroti pentingnya edukasi dan pelatihan dalam meningkatkan kesadaran keamanan siber. Melalui pendekatan ini, individu dapat dipersenjatai dengan pengetahuan yang diperlukan untuk mengidentifikasi dan mengatasi ancaman siber dengan lebih efektif, sehingga meningkatkan keamanan dan perlindungan mereka saat menggunakan layanan dan teknologi digital lainnya (Wathoni et al., 2023).

2.1.5 Knowledge Attitude and Behavior

Dalam konteks keamanan siber, Teori Knowledge, Attitude, and Behavior (KAB) Triandis (1980) memberikan penjelasan tentang bagaimana pengetahuan, sikap, dan perilaku pengguna dapat memengaruhi keamanan informasi dan perlindungan data pribadi. Pengetahuan yang dimiliki pengguna tentang potensi ancaman dan risiko dalam dunia maya dapat memengaruhi sikap mereka terhadap pentingnya perlindungan data dan keamanan siber secara keseluruhan. Misalnya, seseorang yang memiliki pengetahuan tentang cara kerja malware atau phishing akan lebih waspada dan memiliki sikap hati-hati terhadap email atau situs web yang mencurigakan. Dengan pengetahuan yang memadai, sikap positif terhadap praktik keamanan dapat terbentuk, seperti menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara rutin, atau menghindari mengklik tautan yang mencurigakan (Simamora, 2019).

Sikap yang positif terhadap keamanan siber kemudian akan memengaruhi perilaku pengguna dalam dunia maya. Pengguna yang memiliki sikap peduli terhadap keamanan informasi akan lebih cenderung untuk menerapkan langkah-langkah perlindungan yang sesuai, seperti mengaktifkan otentikasi dua faktor, menggunakan perangkat keamanan seperti antivirus, atau tidak membagikan informasi pribadi secara sembarangan. Sebaliknya, individu yang kurang memiliki pengetahuan atau sikap tidak peduli terhadap risiko di dunia maya mungkin akan mengabaikan praktik-praktik keamanan, membuka celah bagi serangan siber. Oleh karena itu, pemahaman tentang hubungan antara pengetahuan, sikap, dan perilaku sangat

penting dalam merancang strategi untuk meningkatkan kesadaran dan memperbaiki praktik keamanan siber di kalangan pengguna internet (Simamora, 2019).

2.1.6 HAIS-Q (*Human Aspects of Information Security Questionnaire*)

Human Aspects of Information Security Questionnaire (HAIS-Q) adalah instrumen yang dikembangkan untuk mengukur kesadaran keamanan informasi di kalangan karyawan dalam suatu organisasi. Instrumen ini menilai tiga komponen utama: pengetahuan tentang kebijakan dan prosedur keamanan informasi, sikap terhadap kebijakan tersebut, dan perilaku aktual dalam penggunaan komputer kerja. Dengan mengevaluasi ketiga aspek ini, HAIS-Q membantu organisasi memahami sejauh mana karyawan mematuhi praktik keamanan informasi yang ditetapkan (Papp & Lovaas, 2021).

Model HAIS-Q (*Human Aspects of Information Security Questionnaire*) dikembangkan dengan mengikuti rekomendasi McGuire (1969), yang menekankan pentingnya pengetahuan sebagai langkah awal. Dalam konteks ini, pengetahuan difokuskan pada 'pengetahuan tentang kebijakan dan prosedur'. Melalui tinjauan terhadap berbagai kebijakan keamanan informasi dan wawancara dengan manajemen senior, dikembangkan tujuh area fokus yang rentan terhadap ketidakpatuhan oleh karyawan dan pengguna komputer. Area tersebut meliputi: penggunaan internet, penggunaan email, penggunaan situs jejaring sosial, manajemen kata sandi (termasuk penguncian workstation), pelaporan insiden, penanganan informasi, dan komputasi *mobile* (Anastasiah & Pandia, 2024).

Untuk setiap area fokus, dikembangkan tiga sub-area yang mewakili perilaku berisiko umum oleh pengguna komputer. Setiap sub-area kemudian dievaluasi melalui satu pertanyaan spesifik yang mengukur pengetahuan, satu pertanyaan yang mengukur sikap, dan satu pertanyaan yang mengukur perilaku. Sebagai contoh, dalam sub-area konsekuensi penggunaan situs jejaring sosial (dalam area fokus penggunaan situs jejaring sosial), pertanyaan yang diajukan adalah:

- a. Pengetahuan: “Saya tidak bisa dipecat karena sesuatu yang saya posting di situs jejaring sosial.”
- b. Sikap: “Adalah ide buruk untuk memposting hal-hal di situs jejaring sosial tentang pekerjaan saya yang tidak akan saya katakan di tempat umum.”
- c. Perilaku: “Saya akan mempertimbangkan konsekuensi negatif terhadap pekerjaan saya sebelum memposting apapun di situs jejaring sosial.”

HAIS-Q telah terbukti sebagai alat yang andal untuk menilai kesadaran keamanan informasi, dengan uji reliabilitas yang menunjukkan konsistensi internal dan stabilitas dari

waktu ke waktu. HAIS-Q digunakan untuk mengidentifikasi area yang memerlukan peningkatan dalam program pelatihan dan kesadaran keamanan informasi, serta untuk mengevaluasi efektivitas intervensi yang telah diterapkan. Dengan demikian, HAIS-Q berperan penting dalam membantu organisasi memitigasi risiko yang terkait dengan perilaku dalam konteks keamanan informasi (Anastasiah & Pandia, 2024).

2.1.7 Analisis Regresi Linear Berganda

Analisis regresi berganda adalah metode yang digunakan untuk memprediksi pengaruh dari dua atau lebih variabel independen terhadap satu variabel dependen. Dengan kata lain, metode ini digunakan untuk menguji ada tidaknya hubungan antara beberapa variabel independen seperti $X_1, X_2, X_3, \dots, X_i$ dengan satu variabel terikat Y . Tujuan utama dari regresi berganda adalah untuk mengetahui apakah terdapat hubungan yang signifikan antara variabel-variabel tersebut dan seberapa besar pengaruh masing-masing variabel independen terhadap variabel dependen.

$$Y = \beta_x + \varepsilon \quad (2.1)$$

Keterangan:

Y = Variabel dependen

β = Parameter

X = Variabel Independen

ε = Error

Secara umum, persamaan analisis regresi dinyatakan sebagai berikut:

$$Y_i = \beta_0 + \beta_1 X_{i1} + \beta_2 X_{i2} + \beta_3 X_{i3} + \varepsilon_i \quad (2.2)$$

Keterangan:

Y_i : variabel dependen untuk pengamatan ke- $i = 1, 2, 3$

$\beta_0, \beta_1, \beta_2$: parameter

X_{i1}, X_{i2}, X_{i3} : variabel independen

ε_i : sisaan (ε) untuk pengamatan ke- i

Menurut Draper dan Smith (1992), hubungan antara satu variabel dependen dengan satu atau lebih variabel independen dapat dijelaskan melalui regresi linier berganda. Hubungan tersebut dirumuskan dalam bentuk persamaan umum.

1. Uji Normalitas

Asumsi persyaratan normalitas harus terpenuhi untuk mengetahui apakah residual/error dari data berdistribusi normal atau untuk mengetahui apakah data sampel berasal dari populasi yang berdistribusi normal. Uji statistik yang digunakan adalah kolmogorov-smirnov. Hipotesis yang digunakan adalah sebagai berikut:

H_0 : data berdistribusi normal

H_1 : data tidak berdistribusi normal

Tingkat signifikan $\alpha = 5\%$

Pengambilan keputusan :

Jika $p\text{-value} < 0,05$ maka H_0 ditolak.

2.1.8 Skala Likert

Menurut (Sugiyono, 2019), Skala Likert digunakan untuk mengukur sikap, pendapat, dan persepsi individu atau kelompok terhadap suatu fenomena sosial. Dalam penggunaannya, variabel yang akan diukur terlebih dahulu diuraikan ke dalam sejumlah indikator. Indikator-indikator tersebut kemudian dijadikan dasar untuk menyusun item-item instrumen dalam bentuk pernyataan atau pertanyaan.

Untuk mengukur variabel dalam penelitian mengenai tingkat kesadaran keamanan siber pada pengguna aktif, peneliti perlu merancang kuesioner yang sesuai dan menggunakan analisis data yang tepat. Desain kuesioner adalah kunci untuk mendapatkan data yang valid dan reliabel. Rancangan kuesioner untuk penelitian tentang tingkat kesadaran keamanan siber pada pengguna aktif dibuat berdasarkan pengukuran variabel dependen dan independen. Hasil kuesioner yang didapatkan akan diukur menggunakan skala Likert. Skala Likert adalah metode pengukuran yang sering digunakan dalam kuesioner untuk menilai tingkat setuju atau tidak setuju responden terhadap pernyataan tertentu. Skala Likert yang digunakan dalam penelitian ini dimuat dalam Tabel 2.1.

Tabel 2. 1 Skala Likert

No	Keterangan	Skor
1	Sangat setuju	5
2	Setuju	4
3	Netral	3
4	Tidak Setuju	2
5	Sangat Tidak Setuju	1

2.1.9 Analisis Deskriptif

Digunakan untuk menggambarkan karakteristik data dan memberikan gambaran umum tentang responden dan variabel yang diteliti, meliputi:

- 1) Mean (rata-rata), dengan rumus 2.3 sebagai berikut:

$$Mean = \frac{\sum_{i=1}^n x_i}{n} \quad (2.3)$$

- 2) Median (nilai tengah), dengan rumus 2.4 sebagai berikut:

$$Median = x_{\frac{(n+1)}{2}} \quad (2.4)$$

- 3) Modus (nilai yang paling sering muncul dalam data.)

- 4) Standar deviasi, dengan rumus 2.5 sebagai berikut:

$$Standar\ Deviasi = \sqrt{\frac{\sum_{i=1}^n (x_i - Mean)^2}{n}} \quad (2.5)$$

Keterangan:

x_i = data ke- i

n = jumlah data

2.2 Penelitian Sebelumnya

Tinjauan pustaka dalam penelitian ini mencakup beberapa penelitian terdahulu seperti pada Tabel 2.2 berikut:

Tabel 2. 2 Penelitian Terdahulu

Judul Penelitian	Metode Penelitian	Hasil Penelitian
Upaya Membangun Kesadaran Keamanan Siber pada Konsumen <i>E-commerce</i> di Indonesia (Nur Rohmah, 2022)	Metode yang digunakan adalah analisis deskriptif berdasarkan data yang diperoleh dari pengamatan, wawancara, serta dokumen yang relevan dengan tema penelitian	Penelitian menunjukkan bahwa kesadaran keamanan siber di kalangan konsumen <i>e-commerce</i> dapat ditingkatkan melalui program kesadaran yang sederhana dan relevan. Program ini memerlukan persiapan struktur, prioritas, materi, penyajian, serta anggaran yang tepat, dengan dukungan penyedia <i>marketplace</i> . Evaluasi berkelanjutan juga penting untuk memastikan keberhasilan program ini.
Analisis Kesadaran Keamanan Siber pada Pengguna Aplikasi <i>E-Court</i> di Lingkungan Pengadilan (Faliandy dkk., 2023)	Metode analisis yang diterapkan adalah deskriptif kuantitatif dengan menggunakan kuesioner sebagai instrumen pengumpulan data	Penelitian menunjukkan bahwa tingkat kesadaran responden dalam penggunaan aplikasi <i>E-Court</i> rendah (42%). Mayoritas responden jarang (73%) atau bahkan tidak pernah (24%) mengganti kata sandi. Namun, kesadaran terhadap penggunaan email (68%) dan kejahatan internet (63%) cukup baik. Pengadilan perlu meningkatkan kesadaran dan pemahaman keamanan siber melalui pendampingan dan edukasi.
Pengaruh Persepsi Manfaat, Persepsi Kemudahan, Dan Persepsi Keamanan Terhadap Keputusan Penggunaan Pada Mahasiswa STIE Bank BPD Jateng (Rahmawati & Yuliana, 2020)	Metode pengumpulan data dilakukan dengan menyebarkan kuesioner secara <i>online</i> . Alat analisis yang digunakan dalam penelitian ini adalah analisis regresi linier berganda	Penelitian menunjukkan bahwa persepsi manfaat, kemudahan, dan keamanan berpengaruh positif dan signifikan terhadap keputusan penggunaan <i>e-wallet</i> di kalangan mahasiswa, dengan persepsi keamanan sebagai faktor paling dominan. Keamanan menjadi sangat penting karena memberikan rasa aman dan terlindungi bagi pengguna.

Berdasarkan beberapa penelitian yang telah dilakukan sebelumnya, penelitian ini dengan judul berupa “Eksplorasi Tingkat Kesadaran Keamanan Siber pada Pengguna Aktif ”. Penelitian ini berfokus pada pengguna aktif di Provinsi Daerah Istimewa Yogyakarta DIY, yang merupakan wilayah dengan pertumbuhan teknologi dan ekonomi yang dinamis. Sebelumnya, penelitian oleh Rahmawati & Yuliana (2020) juga membahas namun pada konteks mahasiswa STIE Bank BPD Jateng, dengan fokus pada persepsi manfaat, kemudahan, dan keamanan yang memengaruhi keputusan penggunaan. Penelitian yang sedang dilakukan akan memperluas pemahaman dengan menjangkau populasi yang lebih umum dan beragam.

Penelitian ini menggunakan metode deskriptif dengan pendekatan kuantitatif serta deskriptif, dan analisis regresi linear berganda untuk menguji faktor-faktor yang memengaruhi tingkat kesadaran keamanan siber pada pengguna . Hal ini memberikan analisis yang lebih mendalam dan komprehensif dibandingkan dengan penelitian oleh Faliandy dkk. (2023) yang menggunakan metode deskriptif kuantitatif dengan kuesioner.

Berbeda dengan penelitian oleh Nur Rohmah (2022) yang menekankan pada program kesadaran keamanan siber untuk konsumen *e-commerce*, penelitian ini khusus meneliti kesadaran keamanan siber di kalangan pengguna aktif . Fokus khusus ini penting karena memiliki karakteristik dan risiko keamanan yang berbeda dengan *platform e-commerce*. Hasil penelitian ini dapat berkontribusi dalam merumuskan kebijakan dan strategi edukasi yang lebih efektif untuk meningkatkan kesadaran keamanan siber di kalangan pengguna . Hal ini sejalan dengan temuan penelitian Faliandy dkk. (2023) yang menunjukkan perlunya pendampingan dan edukasi untuk meningkatkan kesadaran keamanan siber.

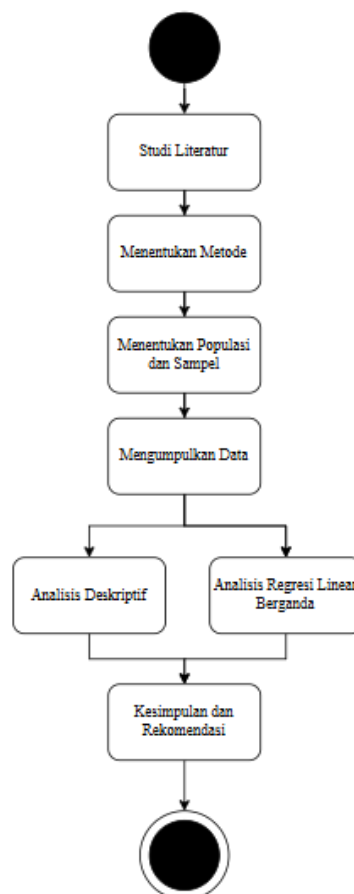
Dengan menggunakan regresi linear berganda, penelitian ini tidak hanya melihat hubungan langsung antara variabel-variabel tetapi juga dapat mengeksplorasi hubungan kausal yang lebih kompleks. Ini memberikan wawasan yang lebih mendalam tentang bagaimana cara berbagai faktor memengaruhi kesadaran keamanan siber, yang belum banyak dieksplorasi dalam penelitian sebelumnya.

Semakin banyaknya transaksi keuangan yang dilakukan secara digital melalui , kesadaran keamanan siber menjadi krusial untuk melindungi pengguna dari ancaman *cyber*. Penelitian ini berupaya untuk mengidentifikasi faktor-faktor yang memengaruhi kesadaran keamanan siber, sehingga dapat memberikan rekomendasi yang lebih tepat sasaran bagi peningkatan keamanan pengguna *e-wallet*.

BAB III

METODOLOGI PENELITIAN

Metodologi penelitian adalah kerangka kerja sistematis yang digunakan oleh peneliti untuk merancang, melaksanakan, dan menganalisis penelitian. Metodologi ini mencakup berbagai langkah dan prosedur yang harus diikuti untuk memastikan bahwa penelitian dilakukan dengan cara yang sah dan dapat dipercaya. Metodologi penelitian menguraikan pendekatan yang akan digunakan dalam mengumpulkan data, menganalisis data, dan menyimpulkan temuan, serta memastikan bahwa proses penelitian dapat direplikasi oleh peneliti lain di masa depan. Metodologi penelitian ini dapat digambarkan dalam diagram alur pada Gambar 3.1.



Gambar 3.1 Diagram Alur Penelitian

Berdasarkan pada alur diagram pada Gambar 3.1, dapat diketahui tahapan-tahapan dalam penelitian ini adalah:

3.1 Studi Literatur

Studi literatur merupakan salah satu tahapan penting dalam penelitian yang bertujuan untuk mengumpulkan dan memahami berbagai referensi teoretis serta data sekunder yang relevan dengan topik penelitian. Menurut Danial dan Warsiah (2009:80), studi literatur dilakukan dengan mengumpulkan informasi dari buku, artikel, jurnal ilmiah, serta dokumen-dokumen lain yang mendukung permasalahan yang diteliti. Dalam penelitian ini, studi literatur dilakukan untuk menggali teori terkait kesadaran keamanan siber, penggunaan *e-wallet*, serta metode yang relevan untuk mengukur kesadaran pengguna terhadap keamanan informasi. Hasil studi literatur menjadi dasar dalam penyusunan kerangka teoretis serta alat ukur, seperti HAIS-Q (Human Aspects of Information Security Questionnaire), yang digunakan dalam penelitian ini.

3.2 Metode Penelitian

Penelitian ini menggunakan metode deskriptif dengan pendekatan kuantitatif. Menurut Sugiyono (2019), penelitian deskriptif bertujuan untuk mengidentifikasi hubungan antara dua atau lebih variabel. Dalam hal ini pendekatan kuantitatif dengan tujuan untuk mengukur tingkat kesadaran keamanan siber pada pengguna aktif *e-wallet* di Daerah Istimewa Yogyakarta DIY. Pendekatan kuantitatif digunakan untuk mengumpulkan informasi dari populasi atau sampel tertentu, menerapkan analisis data, dan menggunakan alat statistik serta instrumen penelitian sebagai sarana pengumpulan data (Sugiyono, 2019).

3.3 Teknik Pengumpulan Data

Pada teknik pengumpulan data, sumber data dalam penelitian ini adalah data primer yang diperoleh langsung melalui penyebaran angket atau kuesioner. Angket atau kuesioner digunakan sebagai teknik pengumpulan data, menghadirkan daftar pernyataan yang harus dijawab oleh responden secara langsung (Sugiyono, 2016). Desain kuesioner disusun untuk mengukur kesadaran terhadap keamanan siber menggunakan pernyataan positif dan negatif, sehingga memudahkan responden dalam memilih jawaban dari opsi yang diberikan. Opsi jawaban diberikan dalam skala Likert, yang menurut Sugiyono (2016), berfungsi sebagai alat ukur untuk persepsi, sikap, dan pendapat individu atau kelompok terhadap suatu fenomena sosial.

3.4 Jenis dan Sumber Data

Penelitian ini merupakan penelitian kuantitatif yang menggunakan data primer. Data primer adalah data yang diperoleh langsung dari responden melalui survei. Survei dilakukan dengan menyebarkan kuesioner secara *online* menggunakan *Google Form* kepada masyarakat yang sesuai dengan kriteria penelitian dan menggunakan . Kuesioner dalam penelitian ini terdiri dari dua puluh pernyataan. Penyusunan pernyataan dari kuesioner ini berdasarkan metode HAIS-Q. HAIS-Q, atau *Human Aspects of Information Security Questionnaire*, adalah metode yang dikembangkan untuk mengukur aspek manusia dalam keamanan informasi. Metode ini berfokus pada tiga komponen utama: pengetahuan (*knowledge*), sikap (*attitude*), dan perilaku (*behavior*) terkait keamanan informasi. Dengan menggunakan HAIS-Q, peneliti dapat mengevaluasi tingkat kesadaran keamanan siber pengguna melalui serangkaian pernyataan yang terstruktur. Pernyataan dan nilai kuesioner dalam penelitian ini disajikan dalam Tabel 1 (lampiran).

3.5 Populasi dan Sampel

Menurut Sugiyono (2016), populasi merujuk pada objek atau subjek dalam suatu wilayah yang memiliki kualitas dan karakteristik tertentu yang akan dianalisis oleh peneliti untuk mencapai kesimpulan. Dalam penelitian ini, populasi yang diidentifikasi adalah pengguna aktif platform di Provinsi Yogyakarta. Sampel dipilih untuk mewakili keseluruhan populasi yang akan diteliti (Sugiyono, 2016). Metode pemilihan sampel yang digunakan adalah *non-probability sampling*, yang memungkinkan setiap anggota populasi tidak memiliki peluang yang sama untuk menjadi sampel. Teknik sampling yang dipilih, yaitu *purposive sampling*, didasarkan pada kriteria spesifik yang ditetapkan peneliti (Taherdoost, 2016), seperti pengguna *platform* dari rentang usia 19 hingga 35 tahun.

Berdasarkan data dari Badan Pusat Statistik (BPS), jumlah penduduk Daerah Istimewa Yogyakarta DIY pada tahun 2024 adalah sekitar 3.759.510 jiwa. Untuk kelompok usia 19 hingga 35 tahun, berikut adalah rincian jumlah penduduk menurut kelompok umur:

- a. Usia 19-24 tahun: 320.406 jiwa
- b. Usia 24-29 tahun: 346.652 jiwa
- c. Usia 30-35 tahun: 322.241 jiwa

Dengan menjumlahkan kelompok usia 19 hingga 35 tahun, jumlah pengguna mencapai total sekitar 989.299 jiwa. Saat ini, penggunaan di Indonesia telah meningkat secara signifikan, dengan sekitar 96% responden dalam survei menyatakan bahwa mereka sudah menggunakan atau memiliki (Muhammad, 2022). Maka, dapat ditentukan jumlah pengguna

untuk kelompok usia 19 hingga 35 tahun di Daerah Istimewa Yogyakarta DIY adalah 96% dari 989.299 adalah sekitar 949.727 jiwa.

Dengan mempertimbangkan *margin of error* sebesar 10% dan tingkat kepercayaan 90% (Rahman, 2023), jumlah sampel ditetapkan dengan menggunakan rumus Solvin pada persamaan 3.1 yaitu :

$$n = \frac{N}{1+N(e)^2} \quad (3.1)$$

Keterangan:

n = Ukuran sampel yang diinginkan

N = Populasi (949.727)

e = *Margin of error* (dalam desimal, yaitu 10% = 0.1)

Maka, diperoleh:

$$n = \frac{949.727}{1 + 949.727 (0.1)^2}$$

$$n = \frac{949.727}{1 + 949.727 \times 0.01}$$

$$n = \frac{949.727}{1 + 9498.27}$$

$$n = \frac{949.727}{9499.27}$$

$$n = 99,9 \text{ (dibulatkan menjadi 100)}$$

Oleh karena itu, nilai sampel yang digunakan dalam penelitian ini adalah 100 orang pengguna untuk kelompok usia 19 hingga 35 tahun di Yogyakarta.

Non-probability sampling, khususnya *purposive sampling*, sering digunakan dalam penelitian yang bertujuan mengeksplorasi fenomena tertentu pada kelompok target yang spesifik. Metode ini mengandalkan penilaian peneliti dalam memilih sampel yang dianggap paling relevan dengan tujuan penelitian (Stratton, 2023).

3.6 Operasional Variabel

Variabel penelitian mengacu pada sekelompok faktor yang peneliti tentukan untuk dikaji dalam suatu penelitian guna mengumpulkan informasi yang relevan. Informasi ini kemudian akan digunakan untuk membuat kesimpulan. Dalam konteks penelitian ini, terdapat dua jenis variabel, yaitu variabel dependen (terikat) dan variabel independen (bebas). Berikut adalah penjelasan untuk masing-masing jenis variabel:

3.6.1 Variabel Dependen

Variabel dependen dalam penelitian ini adalah kesadaran keamanan siber. Kesadaran keamanan siber didefinisikan sebagai tingkat pemahaman, sikap, dan perilaku individu terhadap praktik keamanan informasi dalam penggunaan. Kesadaran ini mencakup pengetahuan tentang ancaman keamanan, sikap terhadap pentingnya perlindungan data, dan perilaku pencegahan serta respons terhadap insiden keamanan. Kesadaran ini diukur melalui tiga komponen utama:

- a. Pengetahuan (*Knowledge*): mencakup pemahaman pengguna tentang konsep dan praktik keamanan siber seperti *phishing*, kata sandi yang kuat, autentikasi dua faktor, risiko penggunaan Wi-Fi publik, tindakan pencegahan terhadap serangan siber, dan risiko keamanan. Pemahaman ini merupakan indikator penting dalam mengevaluasi tingkat kesadaran keamanan siber pengguna (Alotaibi & Alshahrani, 2021).
 1. Pemahaman tentang *phishing*: Seberapa baik pengguna mengenali *email* atau pesan teks yang mencurigakan sebagai upaya *phishing*.
 2. Pemahaman tentang kata sandi yang kuat: Pengetahuan pengguna tentang karakteristik kata sandi yang kuat dan cara membuatnya.
 3. Pemahaman tentang autentikasi dua faktor: Seberapa baik pengguna memahami konsep dan pentingnya autentikasi dua faktor (2FA).
 4. Pemahaman tentang penggunaan WiFi publik: Pengetahuan pengguna bahwa penggunaan WiFi publik untuk transaksi di dapat berisiko.
 5. Pemahaman tentang tindakan pencegahan serangan siber: Pengetahuan pengguna untuk mengambil tindakan jika mengalami serangan siber pada akun .
 6. Pemahaman tentang risiko keamanan: Pengetahuan pengguna tentang risiko keamanan yang terkait dengan penggunaan akun.
- b. Sikap (*Attitude*): meliputi pandangan dan perasaan pengguna terhadap pentingnya keamanan siber dan perlindungan data pribadi. Sikap ini bisa mencakup kepedulian terhadap verifikasi identitas pengirim pesan, pentingnya penggunaan kata sandi yang kuat, kesiapan untuk menggunakan autentikasi dua faktor, pandangan tentang keamanan jaringan, dan kesadaran terhadap risiko serangan siber (Shappie, Stoica, & McDermott, 2021).
 1. Pentingnya memverifikasi identitas pengirim *email*: Seberapa penting pengguna memverifikasi identitas pengirim sebelum membuka *email* dari layanan .

2. Kepedulian terhadap penggunaan kata sandi: Sikap pengguna terhadap penggunaan kata sandi pada akun untuk perlindungan data pribadi mereka.
 3. Kesiapan untuk mengambil tindakan pencegahan: Seberapa bersedia pengguna untuk mengambil langkah-langkah autentikasi dua faktor (2FA) untuk melindungi akun .
 4. Pandangan terhadap keamanan jaringan: Sikap pengguna terhadap penggunaan jaringan Wi-Fi publik dan keamanannya.
 5. Pandangan tentang pencegahan serangan siber: Sikap pengguna yang harus dilakukan jika mengalami serangan siber pada akun .
 6. Kepedulian terhadap risiko keamanan: Sikap pengguna terhadap risiko keamanan yang terkait dengan penggunaan akun .
- c. Perilaku (*Behavior*): mencakup tindakan spesifik yang dilakukan pengguna dalam melindungi akun , seperti verifikasi identitas pengirim pesan, frekuensi mengubah kata sandi, penggunaan autentikasi dua faktor, menghindari Wi-Fi publik, dan tindakan pencegahan terhadap serangan siber. Studi menunjukkan bahwa perilaku ini adalah manifestasi nyata dari kesadaran keamanan siber dan merupakan faktor penentu dalam keamanan digital pengguna (Safa, Solms, & Furnell, 2016).
1. Verifikasi identitas pengirim pesan: Apakah pengguna memverifikasi identitas pengirim sebelum membuka *email* atau pesan yang meminta informasi pribadi.
 2. Frekuensi mengubah kata sandi: Seberapa sering pengguna mengubah kata sandi akun mereka.
 3. Hindari jaringan Wi-Fi publik: Seberapa sering pengguna menghindari penggunaan pada jaringan Wi-Fi publik yang tidak aman.
 4. Penggunaan autentikasi dua faktor: Apakah pengguna mengaktifkan dan menggunakan autentikasi dua faktor pada akun mereka.
 5. Tindakan pencegahan serangan siber: Apakah pengguna mencari informasi atau bantuan jika mengalami serangan siber pada akun .

Menghindari risiko keamanan: Apakah pengguna berhati-hati dan mengambil tindakan pencegahan untuk menghindari risiko keamanan saat menggunakan akun .

3.6.2 Variabel Independen

Variabel independen dalam penelitian ini adalah faktor-faktor yang dapat memengaruhi tingkat kesadaran keamanan siber pada pengguna aktif . Berikut adalah beberapa variabel independen yang diukur dalam penelitian ini:

- a. Umur (*Age*): Kategori usia pengguna .
- b. Pendidikan (*Education*): Tingkat pendidikan pengguna.
- c. Bidang Pekerjaan (*Field of Work*): Bidang pekerjaan pengguna.
- d. Penghasilan Bulanan (*Monthly Income*): Penghasilan bulanan pengguna.
- e. Digunakan (*Used*): Jenis digunakan oleh pengguna.
- f. Paling sering digunakan (*Frequently Used*): yang sering digunakan oleh pengguna.
- g. Frekuensi Penggunaan (*Frequency of Usage*): Seberapa sering pengguna menggunakan .
- h. Sumber Informasi (*Sources of Information*): Sumber informasi yang digunakan oleh pengguna untuk mempelajari tentang keamanan siber, seperti media sosial, berita, atau pelatihan formal.

Variabel independen ini dapat diukur melalui kuesioner yang menanyakan umur, pendidikan, frekuensi penggunaan , dan sumber informasi.

3.7 Analisis Deskriptif

Analisis deskriptif digunakan untuk memberikan gambaran karakteristik responden, seperti usia, pekerjaan, tingkat pendidikan, pendapatan, daerah asal, domisili, dan pengetahuan tentang keamanan siber, berdasarkan respons dari angket atau kuesioner yang disampaikan.

3.8 Analisis Regresi Linear Berganda

Analisis regresi linear berganda adalah metode statistik yang digunakan untuk memahami hubungan antara satu variabel dependen dengan dua atau lebih variabel independen. Metode ini memungkinkan peneliti untuk mengevaluasi seberapa besar pengaruh masing-masing variabel independen terhadap variabel dependen secara simultan. Sehingga dalam pengujiannya menggunakan rumus pada persamaan 2.1.

3.9 Kesimpulan dan Rekomendasi

Bagian akhir adalah penarikan kesimpulan dan rekomendasi, kesimpulan ini merupakan jawaban dari tujuan penelitian, apabila semua tujuan penelitian sudah terjawab pada kesimpulan, berarti penelitian ini sudah benar. Rekomendasi merupakan masukan dari pihak dan sebagai langkah perbaikan pada penelitian selanjutnya.

BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini disajikan hasil penelitian yang telah diperoleh serta pembahasan untuk menganalisis dan menginterpretasikan temuan berdasarkan tujuan penelitian. Penyajian hasil dilakukan secara sistematis sesuai dengan metode yang telah dirancang pada bab sebelumnya. Pembahasan difokuskan untuk mengaitkan hasil dengan teori, penelitian sebelumnya, dan implikasi praktis yang relevan, guna memberikan pemahaman yang mendalam terhadap permasalahan yang dikaji.

4.1 Hasil Analisis Deskriptif

Penelitian ini melibatkan responden dengan beragam latar belakang demografis dan sosial untuk memastikan data yang diperoleh mencerminkan variasi dalam populasi yang diteliti. Tabel 4.1 di bawah berisikan informasi karakteristik 328 orang responden dalam penelitian ini setelah melalui proses pembersihan data. Informasi tersebut disajikan dalam berbagai kategori sesuai informasi demografi yang meliputi Usia, Domisili, Pendidikan, Pekerjaan, dan penghasilan.

Tabel 4.1 Hasil Analisis Deskriptif

Karakteristik		Jumlah	Persen
Usia	18	8	2,4%
	19	7	2,1%
	20	16	4,9%
	21	10	3,0%
	22	22	6,7%
	23	28	8,5%
	24	35	10,7%
	25	23	7,0%
	26	20	6,1%
	27	14	4,3%
	28	19	5,8%
	29	14	4,3%
	30	13	4,0%
	31	13	4,0%
	32	10	3,0%
	33	23	7,0%
	34	10	3,0%
	35	11	3,4%
	36	8	2,4%
	37	11	3,4%
	38	5	1,5%
	39	4	1,2%
	40	2	0,6%

Karakteristik		Jumlah	Persen
	41	1	0,3%
	60	1	0,3%
Domisili	Kabupaten Bantul	47	14,3%
	Kabupaten Gunung Kidul	47	14,3%
	Kabupaten Kulon Progo	51	15,5%
	Kabupaten Sleman	87	26,5%
	Kota Yogyakarta	96	29,3%
Pendidikan Terakhir	SD	1	0,3%
	SMP	1	0,3%
	SMA/SMK	139	42,4%
	Diploma (D1/D2/D3)	49	14,9%
	Sarjana (S1)	136	41,5%
	Magister (S2)	2	0,6%
Pekerjaan	Wiraswasta	100	30,5%
	Karyawan Swasta Consumer Goods	1	0,3%
	Pelajar/Mahasiswa	54	16,5%
	Pemerintahan dan Administrasi Publik (ASN)	48	14,6%
	Pendidikan	34	10,4%
	Penyiar Radio	1	0,3%
	Perbankan dan Jasa Keuangan lainnya	33	10,1%
	Teknologi Informasi & Komunikasi	45	13,7%
	Tidak Bekerja	12	3,7%
Penghasilan	Kurang dari Rp1.000.000	55	16,8%
	Rp1.000.000 - Rp2.999.999	57	17,4%
	Rp3.000.000 - Rp4.999.999	135	41,2%
	Rp5.000.000 - Rp9.999.999	69	21,0%
	Rp10.000.000 - Rp14.999.999	12	3,7%

Karakteristik responden didapatkan dari hasil kuesioner yang sudah disebarkan di berbagai platform sosial media dengan lima variabel demografi Usia, Domisili, Pendidikan Terakhir, Pekerjaan, dan Penghasilan. Dari segi jenis usia, responden didominasi oleh kelompok usia 24 tahun (10,7%) dan 23 tahun (8,5%), menunjukkan bahwa kelompok usia muda paling banyak terwakili. Kelompok usia dengan persentase terendah adalah 41 tahun dan 60 tahun, masing-masing sebesar 0,3%. Sebagian besar responden berada di rentang usia produktif (18–39 tahun), dengan total persentase sebesar 98,5%.

Berdasarkan Domisili, mayoritas responden berasal dari Kota Yogyakarta (29,3%) dan Kabupaten Sleman (26,5%). Domisili dengan persentase terkecil adalah Kabupaten Bantul dan Gunung Kidul, masing-masing sebesar 14,3%. Distribusi domisili ini menunjukkan kecenderungan konsentrasi di daerah perkotaan. Lalu berdasarkan Pendidikan Terakhir, Mayoritas responden memiliki pendidikan SMA/SMK (42,4%) atau Sarjana (S1) (41,5%).

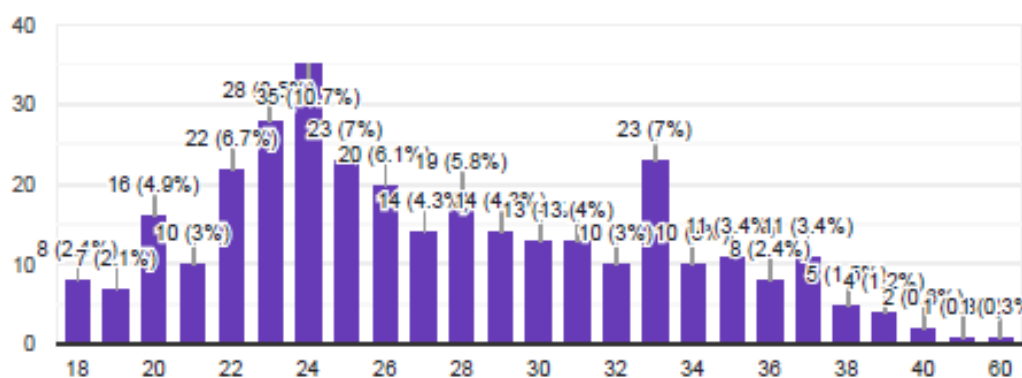
Hanya sedikit responden yang berpendidikan di bawah SMA (0,6%) atau di atas Sarjana (Magister, 0,6%). Hal ini mencerminkan tingkat pendidikan rata-rata responden cukup tinggi.

Berdasarkan profesi, profesi paling dominan adalah wiraswasta (30,5%), diikuti oleh pelajar/mahasiswa (16,5%) dan ASN (14,6%). Profesi dengan jumlah responden paling sedikit adalah penyiar radio dan karyawan swasta, masing-masing hanya 0,3%. Sebagian besar responden aktif bekerja atau menempuh pendidikan. Dari segi penghasilan, sebagian besar responden memiliki penghasilan di rentang Rp3.000.000 – Rp4.999.999 (41,2%), diikuti oleh rentang Rp5.000.000 – Rp9.999.999 (21,0%). Penghasilan terendah (<Rp1.000.000) sebesar 16,8%, sedangkan penghasilan tertinggi (Rp10.000.000–Rp14.999.999) hanya 3,7%. Rata-rata penghasilan responden berada di kategori menengah

Berdasarkan deskripsi dari karakteristik responden dapat disimpulkan bahwa, mayoritas responden adalah individu muda (usia 23–24 tahun), berdomisili di kawasan perkotaan seperti Kota Yogyakarta dan Kabupaten Sleman, dengan tingkat pendidikan SMA/Sl. Profesi dominan adalah wiraswasta, dengan penghasilan sebagian besar berada di rentang Rp3.000.000–Rp4.999.999, menunjukkan responden cenderung aktif secara ekonomi di sektor menengah.

4.1.1 Usia Responden

Berikut persentase usia responden dalam bentuk grafik histogram dapat dilihat pada Gambar 4.1.



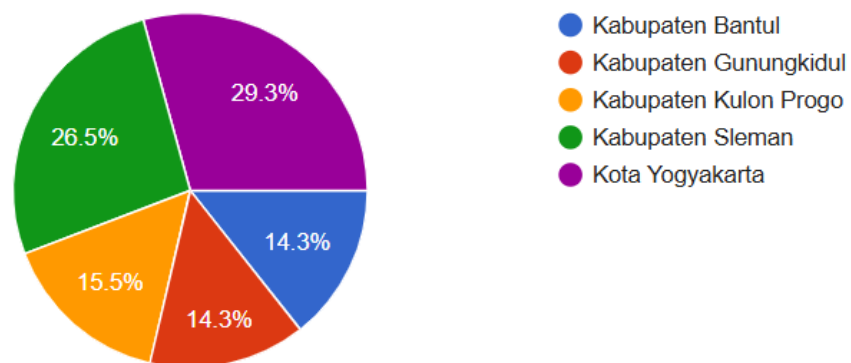
Gambar 4.1 Histogram Usia Responden

Kelompok usia responden menunjukkan dominasi oleh mereka yang berada di rentang usia produktif (18–39 tahun). Berdasarkan data, usia dengan persentase tertinggi: Kelompok usia 24 tahun mencatat jumlah responden terbanyak, yaitu 35 orang (10,7% dari total responden). Disusul oleh usia 23 tahun dengan 28 orang (8,5%). Usia dengan persentase terendah: Kelompok usia 41 tahun dan 60 tahun, masing-masing hanya 1 orang (0,3%).

Rentang usia produktif (18–39 tahun): Mendominasi dengan total 321 responden (98,5%), menunjukkan bahwa survei terutama melibatkan individu dalam usia kerja aktif. Kelompok usia >39 tahun: Terdapat 2 orang (0,6%) dari total populasi. Pengelompokan usia ini menunjukkan bahwa survei lebih banyak melibatkan populasi muda dan dewasa awal, yang dianggap sebagai segmen usia dengan potensi ekonomi dan sosial yang signifikan.

4.1.2 Domisili Responden

Berikut persentase domisili responden berdasarkan asal kabupaten/kota dalam bentuk grafik dapat dilihat pada Gambar 4.2 berikut.

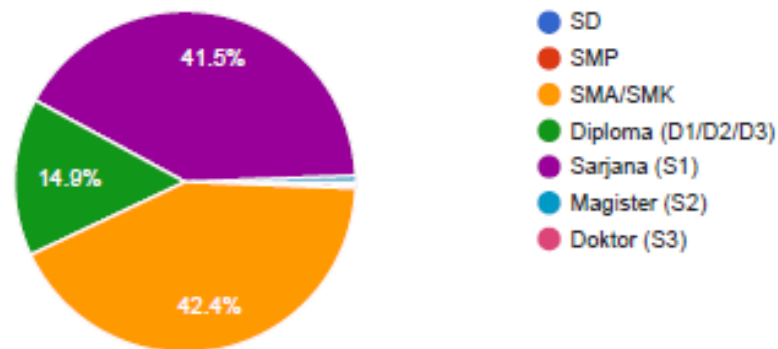


Gambar 4.2 Diagram *Pie* Domisili Responden

Distribusi geografis responden tersebar di wilayah Daerah Istimewa Yogyakarta, dimana Kota Yogyakarta menjadi daerah dengan jumlah responden terbesar, yaitu 96 orang (29,3%), diikuti oleh Kabupaten Sleman sebanyak 87 orang (26,5%). Kabupaten Kulon Progo menempati urutan ketiga dengan 51 orang (15,5%), sementara Kabupaten Bantul dan Kabupaten Gunung Kidul masing-masing tercatat 47 orang (14,3%). Wilayah perkotaan (Kota Yogyakarta dan Kabupaten Sleman) menyumbang 55,8% dari total responden, menunjukkan keterlibatan yang dominan dari area dengan aktivitas ekonomi yang lebih maju dibandingkan daerah pinggiran. Distribusi domisili ini mencerminkan preferensi atau fokus survei terhadap penduduk di pusat kota dan daerah sekitarnya yang lebih berkembang secara ekonomi.

4.1.3 Pendidikan Terakhir

Berikut persentase pendidikan terakhir responden dalam bentuk grafik dapat dilihat pada Gambar 4.3 sebagai berikut.



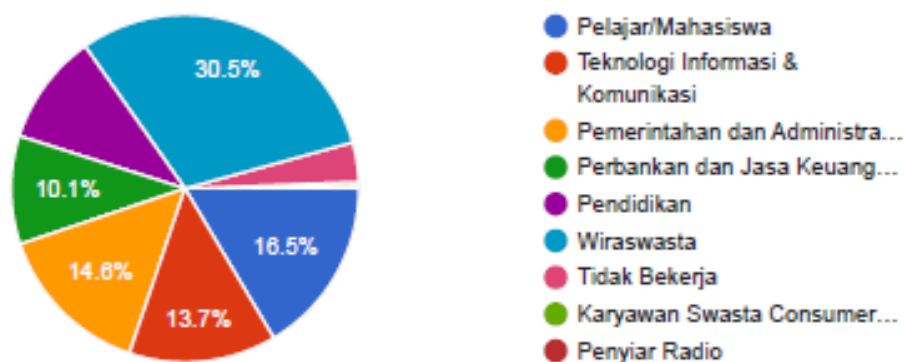
Gambar 4.3 Diagram *Pie* Pendidikan Terakhir Responden

Latar belakang pendidikan responden menggambarkan tingkat pendidikan yang relatif tinggi. Pendidikan menengah atas (SMA/SMK) mendominasi dengan 139 responden (42,4%), diikuti oleh Sarjana (S1) sebanyak 136 orang (41,5%). Diploma (D1/D2/D3) diwakili oleh 49 responden (14,9%), sementara kelompok dengan pendidikan Magister (S2) dan SD/SMP masing-masing hanya 2 orang (0,6%).

Tingkat pendidikan mayoritas menunjukkan bahwa sebagian besar responden memiliki kemampuan dasar dan pengetahuan yang cukup untuk bekerja atau melanjutkan pendidikan lebih tinggi. Mayoritas pendidikan tinggi ini mengindikasikan potensi keterlibatan mereka dalam sektor formal atau semi-formal di dunia kerja

4.1.4 Pekerjaan Responden

Berikut persentase pendidikan terakhir responden dalam bentuk diagram *pie* dapat dilihat pada Gambar 4.4.



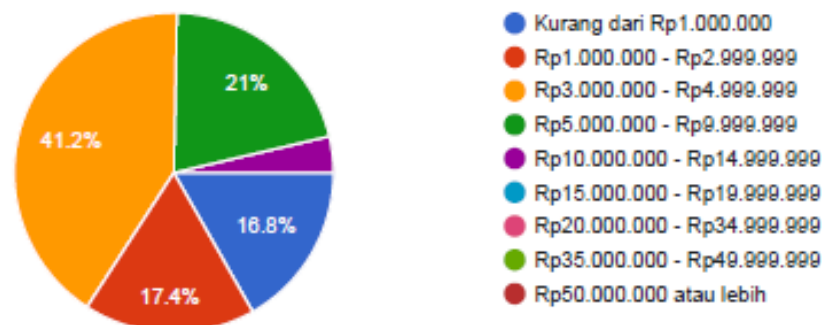
Gambar 4.4 Diagram *Pie* Pekerjaan Responden

Distribusi jenis pekerjaan responden menunjukkan keragaman aktivitas ekonomi, Wiraswasta adalah jenis pekerjaan terbanyak dengan 100 responden (30,5%), mencerminkan minat besar pada usaha mandiri. Pelajar/mahasiswa tercatat sebanyak 54 orang (16,5%), diikuti

oleh pegawai Pemerintahan/ASN sebanyak 48 orang (14,6%). Profesi lainnya seperti sektor teknologi informasi & komunikasi (TIK) melibatkan 45 orang (13,7%), sementara bidang pendidikan memiliki 34 orang (10,4%). Sebagian kecil responden terlibat di sektor perbankan/jasa keuangan (10,1%) atau tercatat sebagai tidak bekerja (3,7%). Keanekaragaman ini menggambarkan keterwakilan responden dari berbagai sektor ekonomi, dengan dominasi pada profesi wiraswasta dan pelajar

4.1.5 Penghasilan Responden

Berikut persentase penghasilan responden dalam bentuk diagram *pie* dapat dilihat pada Gambar 4.5.



Gambar 4.5 Diagram *Pie* Penghasilan Responden

Berdasarkan data, distribusi penghasilan responden menunjukkan kategori ekonomi menengah sebagai yang terbesar yaitu rentang penghasilan Rp3.000.000–Rp4.999.999 adalah yang tertinggi, melibatkan 135 responden (41,2%). Penghasilan Rp5.000.000–Rp9.999.999 berada di urutan kedua dengan 69 orang (21,0%). Penghasilan terendah (<Rp1.000.000) diwakili oleh 55 orang (16,8%), sedangkan penghasilan tertinggi (Rp10.000.000–Rp14.999.999) hanya melibatkan 12 orang (3,7%). Distribusi ini menunjukkan bahwa sebagian besar responden berada di kelas ekonomi menengah dengan pendapatan yang cukup untuk memenuhi kebutuhan hidup sehari-hari.

4.2 Karakteristik Penggunaan *E-wallet*

Penelitian ini melibatkan demografis penggunaan *E-wallet* untuk mengetahui sejauh mana tingkat penggunaan *E-wallet* responden yang mencerminkan variasi dalam populasi yang diteliti. Tabel 4.2 Persentase Karakteristik Penggunaan *E-wallet* di bawah.

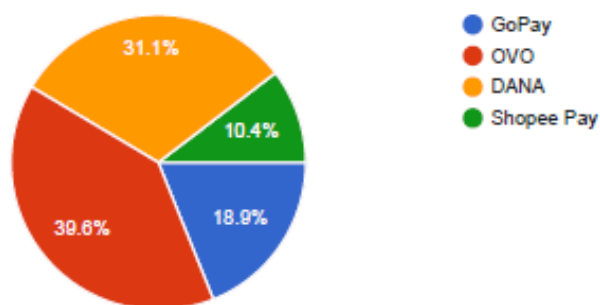
Tabel 4.2 Persentase Karakteristik Penggunaan *E-wallet*

Penggunaan <i>E-wallet</i>		Jumlah	Persen
Jenis <i>E-wallet</i> yang Sering Digunakan	OVO	130	39.63%
	GoPay	62	18.90%
	DANA	102	31.10%
	Shopee Pay	34	10.37%
Frekuensi Penggunaan <i>E-wallet</i> Tertinggi dalam sehari	2 kali	67	20.43%
	3-4 kali	181	55.18%
	5-6 kali	53	16.16%
	Setiap hari	27	8.23%
Sumber Informasi Keamanan Siber	Berita Online	79	24.09%
	Media Sosial	184	56.10%
	Pelatihan Formal	19	5.79%
	Teman atau Keluarga	46	14.02%

Berdasarkan data pada Tabel 4.2, mayoritas responden (70,73%) lebih memilih OVO atau DANA, yang mencerminkan persaingan ketat antara kedua platform ini sebagai pilihan utama pengguna. Selain itu, sebagian besar responden menggunakan *e-wallet* antara 3-6 kali per minggu (71,34%), menandakan bahwa layanan ini telah menjadi bagian integral dari kebutuhan harian mereka. Media sosial menjadi saluran utama edukasi keamanan siber (56,10%), sementara pelatihan formal dimanfaatkan dalam proporsi yang lebih kecil, menunjukkan bahwa edukasi melalui media sosial telah menjadi pendekatan yang dominan dalam meningkatkan kesadaran keamanan siber.

4.2.1 Jenis *E-wallet* yang Sering Digunakan Responden

Berikut persentase Jenis *E-wallet* yang paling sering digunakan oleh responden dalam bentuk diagram *pie* dapat dilihat pada Gambar 4.6 sebagai berikut.

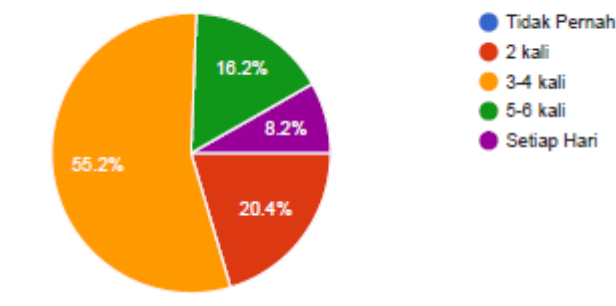
Gambar 4.6 Diagram *Pie* Jenis *E-wallet* Responden

Responden menunjukkan preferensi terhadap beberapa jenis *e-wallet*, dimana OVO adalah yang paling sering digunakan, dipilih oleh 130 responden (39,63%). Popularitasnya bisa dikaitkan dengan kemitraan strategis dengan berbagai layanan, seperti transportasi online atau

platform belanja. DANA menempati urutan kedua, digunakan oleh 102 responden (31,10%). Kemungkinan besar, fitur unggulan dan promosinya menarik bagi pengguna. GoPay dipilih oleh 62 responden (18,90%), menunjukkan bahwa meskipun tidak mendominasi, penggunaannya masih signifikan. Terakhir, ShopeePay adalah aplikasi pembayaran digital dengan penggunaan paling rendah, hanya 34 responden (10,37%). Ini bisa jadi karena ShopeePay lebih spesifik digunakan di dalam ekosistem Shopee

4.2.2 Frekuensi Penggunaan *E-wallet* Tertinggi

Berikut persentase frekuensi Penggunaan *E-wallet* Tertinggi yang digunakan oleh responden dalam bentuk diagram *pie* dapat dilihat pada Gambar 4.7 sebagai berikut.

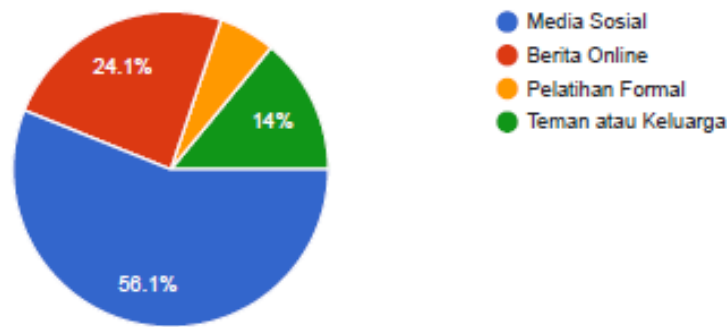


Gambar 4.7 Diagram *Pie* Frekuensi Penggunaan *E-wallet* Responden

Frekuensi penggunaan *e-wallet* memberikan gambaran tentang pola transaksi digital responden, 3-4 kali penggunaan per minggu menjadi yang paling dominan, dipilih oleh 181 responden (55,18%). Ini menunjukkan bahwa mayoritas pengguna menggunakan aplikasi pembayaran digital secara rutin. Dari data diperoleh informasi penggunaan 2 kali per minggu digunakan oleh 67 responden (20,43%), menggambarkan kelompok pengguna dengan tingkat aktivitas sedang. Lalu 5-6 kali per minggu dipilih oleh 53 responden (16,16%), menandakan adanya kelompok pengguna aktif yang hampir setiap hari memanfaatkan *e-wallet*. Penggunaan setiap hari hanya digunakan oleh 27 responden (8,23%), menunjukkan adanya segmen kecil yang sangat bergantung pada pembayaran digital.

4.2.3 Sumber Informasi Keamanan Siber Responden

Berikut persentase Sumber Informasi Keamanan Siber Responden dalam bentuk diagram *pie* dapat dilihat pada Gambar 4.8 sebagai berikut.



Gambar 4.8 *Diagram Pie* Sumber Informasi Keamanan Siber Responden

Responden mendapatkan informasi tentang keamanan siber dari berbagai sumber. Media sosial adalah sumber utama, digunakan oleh 184 responden (56,10%). Ini menunjukkan dominasi platform ini sebagai media edukasi dan informasi. Berita *online* diakses oleh 79 responden (24,09%), menandakan bahwa saluran berita masih relevan untuk informasi keamanan digital. Teman atau keluarga dipilih oleh 46 responden (14,02%), mencerminkan kepercayaan pada sumber informasi langsung dan personal. Pelatihan formal adalah sumber informasi yang paling sedikit digunakan, hanya oleh 19 responden (5,79%), menunjukkan kurangnya partisipasi dalam edukasi keamanan melalui jalur resmi.

4.3 Hasil Skor Kesadaran Keamanan Siber

Dari hasil perhitungan didapatkan nilai yang dapat merepresentasikan tingkat kesadaran keamanan siber, baik secara keseluruhan responden penelitian, individu, maupun kelompok individu yang akan dievaluasi sesuai kriteria yang merupakan hasil penyesuaian dari model Kruger dan Kearney khusus untuk penelitian ini. Adapun kriteria kesadaran yaitu sebagai berikut.

Tabel 4.3 Kriteria Kesadaran

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

Selanjutnya, dilakukan perhitungan skor kesadaran keamanan siber di kalangan pengguna aplikasi pembayaran digital di Yogyakarta yang hasilnya dapat dilihat pada Tabel 4.4 di bawah ini. Skor kesadaran keamanan ini meliputi skor dari masing-masing dimensi dan item yang dijadikan indikator yang kemudian menghasilkan skor akhir kesadaran keamanan secara menyeluruh. Adapun variabel dependen Kesadaran Keamanan Siber didefinisikan sebagai tingkat pemahaman (knowledge), sikap (attitude), dan perilaku individu (behavior) terhadap praktik keamanan informasi dalam penggunaan teknologi. Kesadaran ini mencakup pemahaman mengenai pentingnya penggunaan PIN/Kata Sandi yang kuat untuk melindungi akses terhadap akun dan perangkat, kewaspadaan dalam beraktivitas di internet, termasuk verifikasi identitas pengirim pesan serta kesadaran terhadap ancaman serangan siber, pemahaman mengenai keamanan hardware seperti perangkat penyimpanan data dan akses fisik ke perangkat elektronik, serta kesadaran terhadap software yang digunakan, termasuk pembaruan sistem, perlindungan antivirus, dan risiko penggunaan perangkat lunak bajakan atau tidak terpercaya.

Pertanyaan Kuesioner dibagi berdasarkan dimensi serta item kesadaran yang digunakan yaitu sebagai berikut.

Tabel 4.4 Pernyataan Kuesioner

No.	Pernyataan	Dimensi	Item Kesadaran
1	Verifikasi identitas pengirim diperlukan sebelum membuka email dari layanan e-wallet.	Knowledge	Internet
2	Menggunakan kata sandi yang kuat dan unik untuk setiap akun e-wallet adalah penting.	Knowledge	Pin/Kata Sandi
3	Menggunakan jaringan WiFi publik untuk transaksi di e-wallet tidak memiliki risiko keamanan.	Attitude	Internet
4	Saya memahami konsep dan pentingnya autentikasi dua faktor (2FA).	Knowledge	Pin/Kata Sandi
5	Saya tidak tahu tindakan apa yang harus diambil jika mengalami serangan siber pada akun e-wallet.	Knowledge	Software
6	Saya tahu risiko keamanan yang terkait dengan penggunaan akun e-wallet.	Knowledge	Software
7	Saya merasa penting untuk memverifikasi identitas pengirim sebelum membuka email dari layanan e-wallet.	Attitude	Internet
8	Saya merasa bahwa kata sandi yang tidak unik tetap dapat mengamankan akun e-wallet saya.	Attitude	Pin/Kata Sandi

No.	Pernyataan	Dimensi	Item Kesadaran
9	Saya merasa nyaman menggunakan WiFi publik untuk transaksi di akun e-wallet.	Attitude	Internet
10	Saya merasa bahwa penggunaan autentikasi dua faktor (2FA), untuk melindungi akun e-wallet saya, tidak diperlukan.	Attitude	Pin/Kata Sandi
11	Saya merasa perlu untuk selalu waspada terhadap kemungkinan serangan siber pada akun e-wallet saya.	Attitude	Software
12	Saya merasa bahwa e-wallet selalu aman digunakan tanpa langkah keamanan tambahan.	Attitude	Software
13	Saya terbiasa memverifikasi identitas pengirim sebelum membuka email dari layanan e-wallet.	Behavior	Internet
14	Saya terbiasa menggunakan kata sandi yang sama untuk beberapa akun e-wallet saya.	Behavior	Pin/Kata Sandi
15	Saya terbiasa menghindari menggunakan WiFi publik untuk transaksi di e-wallet.	Behavior	Internet
16	Saya terbiasa mengaktifkan dan menggunakan autentikasi dua faktor pada akun e-wallet saya.	Behavior	Pin/Kata Sandi
17	Saya terbiasa mengambil tindakan pencegahan setelah tahu tentang adanya kemungkinan serangan siber pada akun e-wallet saya.	Behavior	Software
18	Saya terbiasa memastikan keamanan aplikasi e-wallet sebelum menggunakannya untuk transaksi.	Behavior	Software

Dari pernyataan yang telah disusun dan diisi oleh responden diperoleh hasil sebagai berikut.

Tabel 4.5 Tingkat Kesadaran Keamanan Siber

Item	Dimensi			Nilai Kesadaran/ Item
	Knowledge	Attitude	Behavior	
Pin/Kata Sandi	85	85	85	85
Internet	70	67	76	71
Hardware	84	67	81	77
Software	78	76	82	79
Total Kesadaran/ Item	79	74	81	78

Data yang diperoleh menunjukkan tingkat kesadaran keamanan siber secara keseluruhan pada dimensi utama Knowledge (pengetahuan), Attitude (sikap), dan Behavior (perilaku). Analisis lengkap dari setiap komponen dan aspek didasarkan pada skor rata-rata yang diperoleh dari berbagai kategori. Untuk Pin/Kata Sandi Skor Rata-

Rata: 85% (kategori baik). Skor ini menunjukkan bahwa kesadaran akan pentingnya penggunaan pin dan kata sandi sudah berada di tingkat yang baik. Pengguna memahami konsep dasar keamanan terkait perlindungan data dengan autentikasi yang tepat. Walaupun demikian, upaya meningkatkan skor ini tetap diperlukan untuk memastikan konsistensi dan mengantisipasi perkembangan ancaman. Lalu untuk item Internet, skor Rata-Rata: 71% (kategori buruk), kesadaran keamanan dalam penggunaan internet menunjukkan bahwa banyak individu masih belum memahami sepenuhnya risiko yang terkait dengan aktivitas daring, seperti penipuan phishing, malware, atau privasi data. Hal ini menunjukkan perlunya edukasi dan program peningkatan kesadaran, khususnya di segmen ini.

Item Hardware diperoleh Skor Rata-Rata: 77% (kategori buruk), pemahaman terkait keamanan perangkat keras berada di bawah standar yang diharapkan. Hal ini dapat mengindikasikan rendahnya pengetahuan terkait langkah-langkah perlindungan fisik perangkat atau potensi ancaman yang bersumber dari akses fisik perangkat keras. Sama halnya dengan item Software dengan Skor Rata-Rata: 79% (kategori buruk). Kesadaran terhadap keamanan perangkat lunak juga berada pada kategori kurang memadai. Rendahnya skor ini bisa mencakup kurangnya pengetahuan tentang pembaruan perangkat lunak, penggunaan lisensi resmi, dan proteksi dari perangkat lunak berbahaya.

Dari tabulasi yang ada disimpulkan bahwa, Skor Rata-Rata Keseluruhan: 78% (kategori buruk). Dengan skor di bawah ambang batas "baik", ini menunjukkan bahwa tingkat kesadaran keamanan siber pada penggunaan aplikasi pembayaran digital secara keseluruhan masih perlu perhatian khusus. Faktor-faktor ini menunjukkan bahwa meskipun aspek tertentu (seperti perlindungan kata sandi) sudah memadai, masih ada kekurangan signifikan di area lain seperti penggunaan internet, keamanan perangkat keras, dan perangkat lunak. Skor buruk pada aspek seperti internet, perangkat keras, dan perangkat lunak menunjukkan adanya kesenjangan dalam pemahaman dan penerapan keamanan siber. Kampanye edukasi yang menargetkan kelompok rentan perlu segera dilakukan untuk memperbaiki kondisi ini. Meskipun perlindungan pin/kata sandi berada pada tingkat baik, penting untuk memastikan bahwa individu terus mendapatkan informasi terkini tentang metode perlindungan autentikasi yang lebih aman, seperti penggunaan autentikasi dua faktor (2FA).

Secara keseluruhan, tingkat kesadaran keamanan siber berada di kategori yang memerlukan perhatian serius. Dengan rata-rata 78%, upaya terkoordinasi dan strategis

diperlukan untuk meningkatkan pemahaman serta implementasi keamanan di semua dimensi utama. Peningkatan yang konsisten dapat membantu mengurangi risiko dan menciptakan lingkungan digital yang lebih aman bagi individu maupun komunitas.

4.3.1 Skor Kesadaran Keamanan Siber berdasarkan Usia

Berdasarkan data yang dihasilkan dari kuesioner, diperoleh tabulasi skor kesadaran keamanan siber berdasarkan usia pada Tabel 4.5 yaitu sebagai berikut.

Tabel 4.6 Skor Kesadaran Keamanan Siber berdasarkan Usia

Item	Dimensi									Total Kesadaran/Item
	18-27 Tahun			28-39 Tahun			> 39 tahun			
	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	
Pin/Kata Sandi	85	86	79	79	77	87	79	78	83	81
Internet	71	66	85	68	64	77	77	75	85	74
Hardware	85	82	88	70	62	75	82	80	87	79
Software	79	78	75	77	74	75	82	83	76	78
Total Kesadaran/Item	80	78	82	73	69	78	80	79	82	78

Berdasarkan analisis data tingkat kesadaran keamanan siber berdasarkan kategori usia, terdapat perbedaan mencolok di antara kelompok umur yang diteliti. Kelompok usia 18-27 tahun menunjukkan tingkat kesadaran yang cukup baik dengan rata-rata skor total sebesar 80%. Kelompok ini menonjol terutama pada dimensi Behavior dengan skor tertinggi sebesar 82%, yang menunjukkan bahwa generasi muda lebih terampil dalam menerapkan tindakan keamanan siber dalam aktivitas sehari-hari mereka. Hal ini mungkin dipengaruhi oleh tingginya eksposur kelompok usia ini terhadap teknologi digital dan aktivitas daring yang membutuhkan tingkat kewaspadaan lebih tinggi.

Sebaliknya, kelompok usia 28-39 tahun memiliki rata-rata skor total yang lebih rendah, yaitu 73%, yang tergolong dalam kategori buruk. Rendahnya tingkat kesadaran ini menunjukkan adanya kebutuhan untuk memahami lebih lanjut faktor-faktor yang memengaruhi perhatian kelompok ini terhadap praktik keamanan siber. Sementara itu, kelompok usia di atas 39 tahun kembali mencapai skor rata-rata total sebesar 80%, sama seperti kelompok usia termuda. Namun, pencapaian mereka lebih merata di semua dimensi, tanpa dimensi tertentu yang mendominasi. Hal ini menunjukkan bahwa meskipun generasi yang lebih tua mungkin memiliki keterbatasan dalam keahlian teknis, mereka cenderung memiliki pemahaman yang lebih baik tentang pentingnya keamanan data dan lebih berhati-hati dalam bertindak.

Secara keseluruhan, data ini mengindikasikan bahwa tingkat kesadaran keamanan siber tidak linier berdasarkan usia. Kelompok usia muda dan tua menunjukkan performa yang lebih baik dibandingkan kelompok usia menengah. Intervensi yang difokuskan pada kelompok usia 28-39 tahun perlu dilakukan untuk meningkatkan kesadaran mereka, misalnya dengan menyediakan pelatihan keamanan siber yang relevan dengan kebutuhan mereka, baik dalam konteks pekerjaan maupun kehidupan sehari-hari.

4.3.2 Skor Kesadaran Keamanan Siber berdasarkan Domisili

Berdasarkan data yang dihasilkan dari kuesioner, diperoleh tabulasi skor kesadaran keamanan siber berdasarkan domisili yaitu pada Tabel 4.6 sebagai berikut.

Tabel 4.7 Skor Kesadaran Keamanan Siber berdasarkan Domisili

Item	Dimensi															Total Kesadaran/ Item
	Kabupaten Bantul			Kabupaten GunungKidul			Kabupaten Kulon Progo			Kabupaten Sleman			Kota Yogyakarta			
	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Behavior	Knowledge	Attitude	
Pin/Kata Sandi	83	82	80	85	82	81	80	81	80	87	78	80	87	74	75	81
Internet	77	74	79	82	79	83	75	69	75	66	64	76	61	59	73	73
Hardware	89	74	85	85	72	83	84	71	82	83	65	80	82	59	78	78
Software	80	80	82	77	78	82	77	76	79	79	75	82	78	73	84	79
Total Kesadaran/ Item	83	78	81	82	78	82	79	74	79	79	70	80	77	66	77	78

Tingkat kesadaran keamanan siber berdasarkan domisili menunjukkan adanya variasi yang cukup signifikan antarwilayah. Kabupaten Sleman mencatatkan skor rata-rata tertinggi dengan nilai 79%, yang mencerminkan kesadaran yang lebih baik dalam menerapkan langkah-langkah keamanan digital. Hal ini bisa jadi disebabkan oleh tingginya akses terhadap sumber daya pendidikan dan pelatihan di wilayah ini, serta keberadaan institusi teknologi dan komunitas yang mendukung literasi digital. Sleman juga memiliki skor yang baik pada dimensi Attitude, yang menandakan sikap positif terhadap pentingnya keamanan siber dalam kehidupan sehari-hari. Sebaliknya, Kabupaten Kulon Progo menempati posisi terendah dengan skor rata-rata 74%. Skor

ini mencerminkan tingkat kesadaran yang masih perlu ditingkatkan, terutama dalam hal sikap dan perilaku terhadap risiko siber. Rendahnya skor ini mungkin disebabkan oleh keterbatasan infrastruktur teknologi dan kurangnya sosialisasi terkait ancaman digital di wilayah tersebut. Di sisi lain, Kota Yogyakarta menunjukkan keunggulan pada dimensi Behavior dengan skor 84%, yang mengindikasikan bahwa penduduk di wilayah perkotaan lebih sigap dalam mengambil tindakan keamanan untuk melindungi data pribadi mereka. Kota ini juga diuntungkan oleh akses terhadap berbagai pelatihan dan kampanye literasi digital yang lebih mudah diakses dibandingkan wilayah lainnya.

Kabupaten Bantul dan Sleman juga menunjukkan skor yang relatif tinggi pada dimensi Attitude, menandakan kesadaran konseptual yang baik di kalangan masyarakat tentang pentingnya menjaga keamanan informasi. Meski demikian, skor pada dimensi Behavior di wilayah ini belum setinggi Kota Yogyakarta, yang menunjukkan bahwa meskipun masyarakat memiliki pemahaman yang baik, langkah-langkah praktis yang diambil belum sepenuhnya optimal.

Secara keseluruhan, analisis ini mengindikasikan bahwa wilayah dengan akses yang lebih baik terhadap pendidikan, teknologi, dan sumber daya literasi digital cenderung memiliki tingkat kesadaran keamanan siber yang lebih tinggi. Untuk meningkatkan kesadaran di wilayah seperti Kulon Progo, diperlukan intervensi strategis seperti kampanye edukasi berbasis komunitas, peningkatan infrastruktur digital, dan kolaborasi dengan pemerintah daerah untuk meningkatkan literasi siber masyarakat. Pendekatan ini diharapkan dapat menciptakan kesadaran yang merata di seluruh wilayah, mengurangi kesenjangan, dan meningkatkan perlindungan masyarakat terhadap ancaman digital.

4.3.3 Skor Kesadaran Keamanan Siber berdasarkan Pendidikan Terakhir

Berdasarkan data yang dihasilkan dari kuesioner, diperoleh tabulasi skor kesadaran keamanan siber berdasarkan pendidikan terakhir yaitu pada Tabel 4.7 sebagai berikut.

Tabel 4.8 Skor Kesadaran Keamanan Siber berdasarkan Pendidikan Terakhir

Item	Dimensi																		Total Kesadaran/ Item
	SD			SMP			SMA/SMK			Diploma (D1/D2/D3)			Sarjana (S1)			Magister (S2)			
	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	
Pin/Kata Sandi	88	100	88	63	75	63	85	79	78	82	82	83	86	76	78	88	63	63	79
Internet	100	100	100	75	75	75	71	69	78	82	78	78	65	60	74	38	50	75	75
Hardware	75	75	100	50	50	75	85	68	82	87	76	83	82	62	78	75	25	88	73
Software	88	88	75	63	63	50	78	76	81	78	78	80	78	75	84	75	63	81	75
Total Kesadaran/ Item	88	91	91	63	66	66	80	73	80	82	78	81	78	68	79	69	50	77	75

Tingkat kesadaran keamanan siber berdasarkan jenjang pendidikan menunjukkan hasil yang bervariasi, dengan tren yang menarik untuk dianalisis lebih lanjut. Pada tingkat pendidikan SD, skor rata-rata mencapai 91%, yang masuk dalam kategori baik. Hal ini menunjukkan bahwa meskipun masih dalam jenjang pendidikan dasar, peserta survei di kelompok ini memiliki kesadaran yang tinggi terhadap pentingnya keamanan siber. Kemungkinan besar, hasil ini dipengaruhi oleh pendekatan pengajaran yang sederhana namun efektif, atau mungkin pengaruh langsung dari pengawasan orang tua yang turut mendampingi mereka dalam menggunakan teknologi.

Namun, tingkat kesadaran menurun drastis pada jenjang SMP, dengan rata-rata hanya 66%, yang tergolong dalam kategori buruk. Ini mencerminkan adanya celah dalam pemahaman keamanan siber di usia remaja awal, yang mungkin disebabkan oleh transisi ke fase eksplorasi digital yang lebih bebas tanpa pengawasan ketat. Di sisi lain, kelompok SMA/SMK mencatat skor rata-rata 80%, yang menunjukkan peningkatan signifikan dibandingkan tingkat SMP. Hal ini mungkin disebabkan oleh lebih banyaknya program literasi digital atau kurikulum sekolah yang mulai mengenalkan konsep keamanan siber.

Pada tingkat pendidikan tinggi, kelompok Diploma (D1/D2/D3) mencatatkan skor rata-rata 81%, yang sedikit lebih baik dibandingkan Sarjana (79%) dan Magister (77%). Hasil ini menunjukkan bahwa kesadaran keamanan siber cenderung menurun di tingkat pendidikan yang lebih tinggi. Penurunan ini dapat disebabkan oleh perbedaan

fokus di kalangan mahasiswa dan profesional yang lebih sibuk dengan urusan akademik atau pekerjaan sehingga kurang memperhatikan langkah-langkah keamanan digital. Hal ini juga dapat menunjukkan bahwa individu dengan tingkat pendidikan tinggi mungkin merasa terlalu percaya diri terhadap pengetahuan teknis mereka sehingga mengabaikan beberapa tindakan perlindungan dasar.

Secara keseluruhan, analisis ini menunjukkan bahwa tingkat kesadaran keamanan siber tidak sepenuhnya linier dengan tingkat pendidikan. Sementara pendidikan dasar mencatat skor terbaik, peningkatan tingkat pendidikan tidak selalu diikuti dengan peningkatan kesadaran. Oleh karena itu, diperlukan strategi khusus untuk meningkatkan kesadaran keamanan siber di tingkat SMP, serta menanamkan kembali pentingnya praktik keamanan di tingkat Sarjana dan Magister. Program-program berbasis pendidikan formal dan informal, seperti seminar keamanan siber di sekolah dan perguruan tinggi, serta kampanye literasi digital, dapat menjadi solusi yang efektif untuk mengatasi celah ini

4.3.4 Skor Kesadaran Keamanan Siber Berdasarkan Pekerjaan

Berdasarkan data yang dihasilkan dari kuesioner, diperoleh tabulasi skor kesadaran keamanan siber berdasarkan pekerjaan yaitu pada Tabel 4.8 sebagai berikut.

Tabel 4.9 Skor Kesadaran Keamanan Siber berdasarkan Pekerjaan

Item	Dimensi																											
	Karyawan Swasta Consumer Goods			Pelajar/Mahasiswa			Pemerintahan dan Administrasi Publik (ASN)			Pendidikan			Penyiar Radio			Perbankan dan Jasa Keuangan lainnya			Teknologi Informasi & Komunikasi			Tidak Bekerja			Wiraswasta			Total Kesadaran/ Item
	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	
Pin/Kata Sandi	88	63	50	86	72	70	84	79	78	82	74	73	75	50	75	84	75	79	88	77	82	91	91	89	84	83	84	78
Internet	25	25	100	56	57	70	70	71	78	65	66	70	50	50	75	67	63	80	66	61	72	88	79	88	80	73	81	68
Hardware	75	25	100	82	57	78	80	68	79	86	62	82	75	50	50	83	61	74	83	60	78	94	77	98	86	77	85	74
Software	75	63	88	78	73	84	77	75	81	74	73	81	63	75	75	80	73	80	76	74	84	84	84	84	80	80	81	78
Total Kesadaran / Item	66	44	84	76	65	75	78	74	79	77	69	76	66	56	69	78	68	78	78	68	79	89	83	90	83	78	83	74

Tingkat kesadaran keamanan siber berdasarkan kategori pekerjaan menunjukkan variasi yang mencerminkan pengaruh profesi terhadap pemahaman, sikap, dan tindakan dalam menjaga keamanan digital. Kategori pekerjaan dengan skor tertinggi adalah kelompok Perbankan dan Jasa Keuangan Lainnya, yang mencatat rata-rata sebesar 89%. Hasil ini menunjukkan bahwa sektor perbankan memiliki tingkat kesadaran yang sangat baik, kemungkinan besar karena sifat pekerjaan mereka yang menuntut pengelolaan data sensitif dan eksposur terhadap regulasi ketat terkait keamanan informasi. Pekerja di sektor ini umumnya mendapatkan pelatihan intensif mengenai prosedur keamanan digital, termasuk perlindungan terhadap ancaman siber seperti phishing, peretasan akun, dan pencurian identitas.

Kelompok pekerja di bidang Teknologi Informasi dan Komunikasi juga mencatat skor yang baik, terutama pada dimensi Knowledge dengan nilai 84% dan Behavior sebesar 79%. Hal ini dapat dijelaskan oleh tingkat keakraban mereka dengan teknologi dan pemahaman mendalam tentang potensi risiko yang terkait dengan infrastruktur digital. Meskipun skor mereka tidak setinggi sektor perbankan, pekerja di bidang ini memiliki kesadaran praktis yang cukup kuat, meskipun masih ada ruang untuk meningkatkan aspek sikap (Attitude), yang dapat mencerminkan kebutuhan untuk lebih mengintegrasikan pemahaman teoritis dan etika keamanan dalam rutinitas kerja mereka.

Sebaliknya, kategori Tidak Bekerja memiliki skor rata-rata yang rendah, yaitu 69%, yang tergolong dalam kategori buruk. Rendahnya tingkat kesadaran ini kemungkinan dipengaruhi oleh kurangnya akses terhadap pelatihan keamanan digital yang biasanya tersedia di lingkungan kerja formal. Keterbatasan pengetahuan dan kesadaran akan pentingnya keamanan siber pada kelompok ini dapat membuat mereka lebih rentan terhadap ancaman siber, seperti pencurian data atau penyalahgunaan informasi pribadi.

Secara keseluruhan, analisis ini menunjukkan bahwa jenis pekerjaan memiliki pengaruh signifikan terhadap tingkat kesadaran keamanan siber. Pekerjaan yang secara langsung terkait dengan data sensitif dan teknologi cenderung memiliki tingkat kesadaran yang lebih baik dibandingkan kelompok yang tidak bekerja atau yang berada di sektor dengan risiko siber lebih rendah. Oleh karena itu, penting untuk memperluas pelatihan keamanan siber ke berbagai sektor pekerjaan, termasuk melalui program pelatihan bagi kelompok masyarakat yang tidak bekerja. Dengan demikian, kesadaran

keamanan digital dapat ditingkatkan secara menyeluruh di berbagai lapisan masyarakat, mengurangi risiko serangan siber yang terus berkembang.

4.3.5 Skor Kesadaran Keamanan Siber Berdasarkan Penghasilan

Berdasarkan data yang dihasilkan dari kuesioner, diperoleh tabulasi skor kesadaran keamanan siber berdasarkan penghasilan yaitu pada tabel 4.9 sebagai berikut.

Tabel 4.10 Skor Kesadaran Keamanan Siber berdasarkan Penghasilan

Item	Dimensi															Total Kesadaran/ Item
	Kurang dari Rp1.000.000			Rp1.000.000 - Rp2.999.999			Rp3.000.000 - Rp4.999.999			Rp5.000.000 - Rp9.999.999			Rp10.000.000 - Rp14.999.999			
	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Knowledge	Attitude	Behavior	Behavior	Knowledge	Attitude	
Pin/Kata Sandi	86	76	73	85	84	83	84	83	85	86	69	70	88	60	64	78
Internet	60	60	74	79	77	85	83	76	78	51	50	70	33	40	67	66
Hardware	83	60	82	92	74	86	86	78	85	78	49	70	60	40	69	73
Software	79	75	84	78	79	80	80	79	80	74	68	86	74	66	88	78
Total Kesadaran/ Item	77	68	78	83	78	83	83	79	82	72	59	74	64	51	72	74

Berdasarkan data, terdapat variasi kesadaran keamanan siber berdasarkan kelompok penghasilan. Kelompok dengan penghasilan kurang dari Rp1.000.000 menunjukkan total kesadaran sebesar 78%, dengan skor tertinggi pada dimensi behavior (83%) dan skor terendah pada knowledge (77%). Kelompok penghasilan Rp1.000.000 - Rp2.999.999 memiliki total kesadaran yang sama, yaitu 78%, dengan behavior tetap mendominasi (83%) dan attitude berada di posisi terendah (68%). Pada kelompok Rp3.000.000 - Rp4.999.999, total kesadaran mencapai skor tertinggi, yaitu 79%, dengan dimensi knowledge berada di angka tertinggi (86%) dan attitude menjadi yang terendah (64%). Namun, kesadaran mulai menurun pada kelompok penghasilan Rp5.000.000 - Rp9.999.999 dengan total skor 74%, di mana knowledge mendominasi (78%) dan baik attitude maupun behavior sama-sama memiliki skor terendah (64%). Penurunan ini berlanjut pada kelompok penghasilan Rp10.000.000 - Rp14.999.999 dengan total kesadaran 73%, yang menjadi skor terendah di antara semua kelompok, dengan knowledge memiliki skor tertinggi (75%) dan attitude terendah (60%).

Secara keseluruhan, dimensi knowledge secara konsisten memiliki skor lebih tinggi dibandingkan dimensi lainnya di hampir semua kelompok penghasilan, menunjukkan bahwa pengetahuan tentang keamanan siber relatif terdistribusi dengan baik. Sebaliknya, dimensi attitude sering kali memiliki skor terendah, menandakan adanya tantangan dalam membangun sikap positif terhadap keamanan digital.

4.4 Hasil Analisis Regresi Berganda

Selanjutnya yaitu dilakukan analisis Regresi Berganda, analisis regresi linear berganda yang bertujuan untuk mencari faktor-faktor demografis yang berpengaruh pada perbedaan tingkat kesadaran keamanan siber pengguna *e-wallet* di Yogyakarta. Variabel independen meliputi Knowledge (pengetahuan), Attitude (sikap), dan Behavior (perilaku), sedangkan variabel dependen adalah berbagai aspek demografis, seperti usia, domisili, pendidikan terakhir, pekerjaan, dan penghasilan. Adapun hasil dari setiap variabel yaitu sebagai berikut.

Tabel 4.11 Hasil Olah Data Regresi Linear Variabel Usia

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1,587	,307		5,162	,000
	Knowledge	,047	,097	,029	,481	,631
	Attitude	-,067	,078	-,057	-,859	,391
	Behavior	-,023	,096	-,015	-,238	,812

a. Dependent Variable: Usia

Dari Tabel 4.10 diketahui bahwa, konstanta memiliki nilai sebesar 1,587 ($p < 0,001$), yang menunjukkan bahwa tanpa memperhitungkan variabel independen, tingkat kesadaran siber memiliki pengaruh signifikan. Ketiga variabel independen (Knowledge, Attitude, dan Behavior) tidak memiliki pengaruh signifikan terhadap usia, dengan nilai Sig. masing-masing 0,631, 0,391, dan 0,812. Dengan demikian, usia tidak dipengaruhi secara signifikan oleh tingkat pengetahuan, sikap, maupun perilaku terkait keamanan siber.

Tabel 4.12 Hasil Olah Data Regresi Linear Variabel Domisili

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.461	.727		6.138	.000
	Knowledge	.176	.230	.045	.766	.444
	Attitude	-.892	.183	-.309	-4.867	.000
	Behavior	.276	.227	.075	1.217	.225
a. Dependent Variable: Domisili						

Konstanta memiliki nilai 4.461 ($p < 0,001$), menunjukkan tingkat kesadaran yang signifikan. Attitude memiliki pengaruh negatif signifikan (Beta = -0,309, $p = 0,000$), menandakan bahwa sikap yang lebih baik cenderung dikaitkan dengan faktor domisili tertentu. Variabel Knowledge dan Behavior tidak menunjukkan pengaruh signifikan terhadap domisili, dengan nilai Sig. masing-masing 0,444 dan 0,225.

Tabel 4.13 Hasil Olah Data Regresi Linear Variabel Pendidikan Terakhir

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.705	.502		7.383	.000
	Knowledge	.212	.159	.080	1.339	.182
	Attitude	-.408	.127	-.209	-3.225	.001
	Behavior	.260	.156	.104	1.662	.098
a. Dependent Variable: Pendidikan Terakhir						

Pendidikan Terakhir sebagai Variabel Dependen, diperoleh hasil konstanta sebesar 3.705 signifikan ($p < 0,001$). Sikap (Attitude) memiliki pengaruh negatif signifikan (Beta = -0,209, $p = 0,001$), menunjukkan hubungan terbalik antara sikap dan pendidikan terakhir. Pengetahuan (Knowledge) dan perilaku (Behavior) tidak signifikan terhadap pendidikan terakhir ($p > 0,05$).

Tabel 4.14 Hasil Olah Data Regresi Linear Variabel Pekerjaan

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.403	1.412		3.118	.002
	Knowledge	.442	.446	.060	.991	.322
	Attitude	-.877	.356	-.161	-2.464	.014
	Behavior	.238	.440	.034	.541	.589

a. Dependent Variable: Pekerjaan

Konstanta memiliki nilai 4.403 yang signifikan ($p = 0,002$). Sikap (Attitude) menunjukkan pengaruh negatif signifikan ($Beta = -0,161$, $p = 0,014$), yang menunjukkan bahwa sikap yang lebih baik berhubungan dengan jenis pekerjaan tertentu. Knowledge dan Behavior tidak menunjukkan pengaruh signifikan terhadap pekerjaan ($p > 0,05$).

Tabel 4.15 Hasil Olah Data Regresi Linear Variabel Penghasilan

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.052	.563		7.202	.000
	Knowledge	-.015	.178	-.005	-.085	.933
	Attitude	-.464	.142	-.211	-3.267	.001
	Behavior	-.008	.175	-.003	-.047	.962

a. Dependent Variable: Penghasilan

Konstanta sebesar 4.052 signifikan ($p < 0,001$). Sikap (Attitude) memiliki pengaruh negatif signifikan ($Beta = -0,211$, $p = 0,001$), menunjukkan bahwa sikap berhubungan dengan tingkat penghasilan. Pengetahuan (Knowledge) dan perilaku (Behavior) tidak memiliki pengaruh signifikan ($p > 0,05$).

Hasil analisis menunjukkan bahwa sikap (Attitude) adalah variabel independen yang paling konsisten memengaruhi berbagai aspek demografis, khususnya domisili, pendidikan terakhir, pekerjaan, dan penghasilan. Namun, pengetahuan (Knowledge) dan perilaku (Behavior) tidak memberikan pengaruh signifikan terhadap semua aspek demografis yang dianalisis.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai kesadaran keamanan siber pengguna *e-wallet* di Yogyakarta, dapat disimpulkan sebagai berikut:

1. Berdasarkan hasil penelitian, tingkat kesadaran keamanan siber pengguna *e-wallet* di Daerah Istimewa Yogyakarta secara keseluruhan masih berada dalam kategori cukup baik, tetapi belum optimal. Dari hasil analisis menggunakan metode Human Aspects of Information Security Questionnaire (HAIS-Q), ditemukan bahwa rata-rata skor kesadaran keamanan siber mencapai 78%, yang berarti sebagian besar pengguna memiliki pemahaman dasar mengenai ancaman keamanan siber, tetapi masih terdapat beberapa aspek yang perlu ditingkatkan. Dalam aspek Knowledge (pengetahuan) dan Behavior (perilaku), pengguna menunjukkan tingkat kesadaran yang lebih tinggi dibandingkan dengan Attitude (sikap). Hal ini mengindikasikan bahwa sebagian besar pengguna telah memahami ancaman keamanan seperti phishing, malware, dan pencurian identitas, serta telah menerapkan beberapa tindakan perlindungan dasar seperti penggunaan PIN yang kuat dan menghindari tautan mencurigakan. Namun, aspek Attitude (sikap) masih menjadi kelemahan utama dalam kesadaran keamanan siber. Banyak pengguna masih memiliki persepsi yang kurang serius terhadap risiko keamanan siber. Seperti, sekitar 32% responden masih cenderung menggunakan kata sandi yang sama untuk berbagai akun, sementara 47% pengguna masih menyimpan informasi sensitif seperti nomor kartu kredit di perangkat mereka tanpa perlindungan tambahan. Kesadaran terhadap pentingnya pembaruan perangkat lunak dan pemanfaatan autentikasi dua faktor (2FA) juga masih tergolong rendah.
2. Hasil analisis regresi menunjukkan bahwa faktor Attitude (sikap) memiliki pengaruh yang paling signifikan terhadap kesadaran keamanan siber di berbagai aspek demografi, termasuk domisili, pendidikan terakhir, pekerjaan, dan penghasilan. Pengguna di daerah perkotaan seperti Sleman dan Kota Yogyakarta memiliki tingkat kesadaran yang lebih tinggi dibandingkan mereka yang berada di daerah pinggiran seperti Kulon Progo dan Gunung Kidul. Pendidikan juga menjadi faktor yang memengaruhi, di mana pengguna dengan tingkat pendidikan lebih tinggi (Sarjana dan Magister) memiliki kesadaran keamanan siber yang lebih baik dibandingkan mereka dengan pendidikan menengah ke

bawah. Pekerjaan dan Penghasilan menunjukkan bahwa pengguna yang bekerja di sektor teknologi informasi dan keuangan memiliki tingkat kesadaran yang lebih baik dibandingkan pekerja di sektor informal. Adapun sumber informasi yang paling banyak digunakan adalah media sosial (56,10%), sementara pelatihan formal hanya diakses oleh 5,79% pengguna, menunjukkan bahwa edukasi formal tentang keamanan siber masih sangat minim.

5.2 Saran

Sebagai langkah untuk meningkatkan tingkat kesadaran keamanan siber di kalangan pengguna *e-wallet*, diperlukan upaya yang terintegrasi dari berbagai pihak, termasuk pemerintah, penyedia layanan *e-wallet*, dan masyarakat. Berikut adalah beberapa saran yang dapat menjadi rekomendasi strategis yaitu sebagai berikut.

1. Peningkatan Edukasi Keamanan Siber, Pemerintah dan penyedia *e-wallet* perlu bekerja sama untuk mengadakan kampanye edukasi berbasis komunitas dan pelatihan keamanan siber, terutama di daerah pinggiran seperti Kulon Progo dan Gunung Kidul. Meningkatkan konten edukasi melalui media sosial yang sering diakses pengguna, namun tetap memperkuat jalur pelatihan formal untuk menciptakan pemahaman yang lebih mendalam.
2. Media sosial sebagai sumber informasi perlu dikelola secara lebih efektif, dengan menyediakan informasi yang terverifikasi dan relevan mengenai ancaman keamanan terbaru. Menambah program literasi digital di sekolah dan perguruan tinggi, khususnya pada jenjang SMP hingga SMA/SMK, untuk membangun kebiasaan proteksi siber sejak dini.
3. Penyedia layanan *e-wallet* perlu mengintegrasikan fitur keamanan canggih, seperti autentikasi dua faktor (2FA), deteksi anomali transaksi, dan notifikasi real-time untuk aktivitas mencurigakan. Pemerintah perlu memperkuat regulasi terkait perlindungan data pengguna dan memberikan sanksi yang jelas terhadap pelanggaran keamanan oleh penyedia layanan.
4. Kampanye khusus perlu menyasar kelompok dengan skor kesadaran rendah, seperti pengguna dengan penghasilan rendah atau yang tidak bekerja, untuk memperluas jangkauan literasi keamanan siber. Meningkatkan akses ke perangkat lunak keamanan yang terjangkau atau gratis, serta menyediakan informasi langkah-langkah pencegahan sederhana yang dapat dilakukan oleh semua pengguna.

DAFTAR PUSTAKA

- Aaputra, S. A., Didi Rosiyadi, Windu Gata, & Syepri Maulana Husain. (2019). Sentiment Analysis Analysis of *E-wallet* Sentiments on Google Play Using the Naive Bayes Algorithm Based on Particle Swarm Optimization. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 3(3), 377–382. <https://doi.org/10.29207/resti.v3i3.1118>
- Alif, M. S., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan di Kalangan Pengguna *E-wallet* di Indonesia. *Jurnal Informasi*, 2(1), 1–7. Retrieved from <https://journal.uui.ac.id/AUTOMATA/article/view/17279>
- Alotaibi, M. A., & Alshahrani, M. A. (2021). Awareness of cybersecurity issues among *e-wallet* users: A Saudi Arabian study. *Journal of Information Security and Applications*, 59(10), 28–70. Retrieved from <https://doi.org/10.1016/j.jisa.2021.102870>
- Anastasiah, M., & Pandia, H. (2024). Analisis Perilaku Pengguna Mobile Banking Terhadap Keamanan Informasi Menggunakan Metode Human Aspects of Information Security Questionnaire (HAIS-Q). *Innovative: Journal Of Social Science Research*, 4(2), 4067–4078. <https://doi.org/10.31004/innovative.v4i2.9684>
- Anjani, D., Awali, H., & Misidawati, D. N. (2022). Analisis Faktor-Faktor Yang Memngaruhi Minat Generasi Z Dalam Menggunakan Sistem Pembayaran *E-wallet*. *Jurnal Sahmiyya*, 1(1), 124–134. Retrieved from www.dana.id,
- Arfan Dwi Madya, Bagas Djoko Haryanto, & Devi Putri Ningsih. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *Indonesian Journal of Education And Computer Science*, 1(3), 127–135. <https://doi.org/10.60076/indotech.v1i3.236>
- Carrasco, J. L. (2009). Structural Equation Model. *Media Informatika*, 8(3), 1300–1305. <https://doi.org/10.3109/9781439822463.209>
- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 10(2), 113–128. <https://doi.org/10.22212/jp.v10i2.1447>
- Ekonomi, W. (2019). Apa itu Dompot Digital. Retrieved from Warta Ekonomi website: <http://www.wartaekonomi.co.id/>
- Faliandy, M Yonandio Lazuardi, & Tata Sutabri. (2023). Analisis Kesadaran Keamanan Siber pada Pengguna Aplikasi E-Court di Lingkungan Pengadilan. *Jurnal Ilmiah Binary STMIK*

- Bina Nusantara Jaya Lubuklinggau*, 5(2), 101–107. <https://doi.org/10.52303/jb.v5i2.106>
- Harminingtyas, R., Susetyarsi, T., Pengaruh Persepsi Kemudahan, Persepsi Manfaat, dan P., Keamanan Terhadap Pengguna *E-wallet* di Masyarakat kota, Semarang, Tinggi, S., ... Semarang, S. (2020). Pengaruh Persepsi Manfaat, Persepsi Kemudahan dan Persepsi Keamanan terhadap Pengguna *E-wallet* Pada Masyarakat Di Kota Semarang. *Jurnal Ilmiah Fokus Ekonomi, Manajemen, Bisnis Dan Akuntansi*, (2829–1433), 390.
- Hoshmand, M. O., Ratnawati, S., & Korespondensi, E. P. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Jurnal Sains Dan Teknologi*, 5(2), 679–686. Retrieved from <https://doi.org/10.55338/saintek.v5i2.2347>
- Indonesia, B. (2016). *Peraturan Bank Indonesia Nomor 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran*. Jakarta: Bank Indonesia.
- Kusnawan, A., Diana, S., Andy, A., & Tjong, S. (2019). Pengaruh Diskon pada Aplikasi *e-wallet* terhadap Pertumbuhan Minat Pembelian Impulsif Konsumen Milenial di Wilayah Tangerang. *Sains Manajemen*, 5(2), 137–160. <https://doi.org/10.30656/sm.v5i2.1861>
- Muhammad, P. W. (2022). *Analisis Penggunaan Kalangan Generasi Z di Yogyakarta Dengan Pendekatan Techonolgy Acceptance Model (TAM)*.
- Nur Rohmah, R. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Cendekia Niaga*, 6(1), 1–11. <https://doi.org/10.52391/jcn.v6i1.629>
- Papp, G., Lovaas, P. (2021). Assessing Small Institutions' Cyber Security Awareness Using Human Aspects of Information Security Questionnaire (HAIS-Q). In: Arai, K. (eds) *Intelligent Computing. Lecture Notes in Networks and Systems*, vol 285. Springer, Cham. https://doi.org/10.1007/978-3-030-80129-8_62
- Rahman, M. M. (2023). Sample Size Determination for Survey Research and Non-Probability Sampling Techniques: A Review and Set of Recommendations. *Journal of Entrepreneurship, Business and Economics*, 11(1), 42–62. Retrieved from www.scientificia.com
- Rahmawati, Y. D., & Yuliana, R. (2020). Pengaruh Persepsi Manfaat, Persepsi Kemudahan, Dan Persepsi Keamanan Terhadap Keputusan Penggunaan *E-wallet* Pada Mahasiswa Stie Bank Bpd Jateng. *Econbank*, 2(2), 157–168. Retrieved from <https://www.liputan6.com>
- Safa, N. S., Solms, R. von, & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70–82. Retrieved from

<https://doi.org/10.1016/j.cose.2015.10.006>

- Shappie, A. T., Stoica, M., & McDermott, H. (2021). Cybersecurity awareness and behavior among young adults: A case study of mobile payments and *e-wallets*. *Journal of Information Systems Applied Research*, 14(3), 12–25.
- Stratton, S. J. (2023). Population Sampling: Probability and Non-Probability Techniques. *Prehospital and Disaster Medicine*, 38(2), 147–148.
<https://doi.org/10.1017/S1049023X23000304>
- Susanti, N. L. P. R., & Dwiana Putra, I. M. P. (2023). Pengaruh Persepsi Kemudahan, Kualitas Layanan, Dan Risiko Keamanan Terhadap Keputusan Penggunaan *E-wallet* Dalam Transaksi Keuangan. *E-Jurnal Ekonomi Dan Bisnis Universitas Udayana*, 12(03), 407.
<https://doi.org/10.24843/eeb.2023.v12.i03.p05>
- Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for. *International Journal of Academic Research in Management (IJARM)*, 5(2), 18–27.
- Umiyati, I., Eka Putri, T., Maya, N., Artikel, I., & Artikel, H. (2021). Social Influence, Usability And Security On The Intensity of DANA *e-wallet* Use. *Journal of Accounting for Sustainable Society (JASS)*, 03, 113–130.
- Wathoni, M., Efendi, Y., Maulana, A., Anfa, E. N., Alegra, V. P., Rifki, M., & Fauzan, A. (2023). Kesadaran Keamanan Siber (Cyber Security Awareness) Pada Smp Labschool Fip Umj. *Jurnal Universitas Muhammadiyah Jakarta*, Volume 2(No 3). Retrieved from <http://jurnal.umj.ac.id/index.php/semnaskat>
- Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., & Rizkianfi, M. W. (2023). Analisis Potensi Dan Strategi Pencegahan Cyber Crime Dalam Sistem Logistik Di Era Digital. *Jurnal Bisnis, Logistik Dan Supply Chain (BLOGCHAIN)*, 3(1), 23–32.
<https://doi.org/10.55122/blogchain.v3i1.714>

LAMPIRAN

Tabel 1. Pernyataan dan Nilai Kuesioner

No	Komponen	Pernyataan	Nilai
1.	Demografi & Pertanyaan untuk Menggali Variabel Independen	Apakah anda berdomisili di Yogyakarta saat ini?	Ya Tidak
2.		Berapakah usia anda saat ini?	Di isi oleh pengguna
3.		Domisili Anda saat ini?	Kabupaten Bantul Kabupaten Gunungkidul Kabupaten Kulon Progo Kabupaten Sleman Kota Yogyakarta
4.		Tingkat pendidikan terakhir anda?	SD SMP SMA/SMK Diploma (D1/D2/D3) Sarjana (S1) Magister (S2) Doktor (S3)
5.		Bidang Pekerjaan?	Pelajar/Mahasiswa Teknologi Informasi & Komunikasi Pemerintahan dan Administrasi Publik (ASN) Perbankan dan Jasa Keuangan lainnya Pendidikan Wiraswasta Tidak Bekerja Other
6.		Penghasilan Bulanan?	Kurang dari Rp, 1,000,000 Rp, 1,000,000 - 3,000,000 Rp, 3,000,000 - 4,000,000 Rp, 5,000,000 - 9,000,000 Rp, 10,000,000 - 14,000,000 Rp, 15,000,000 - 19,000,000 Rp, 20,000,000 - 34,000,000 Rp, 35,000,000 - 49,000,000 Rp, 50,000,000 atau lebih
7.		Apa saja yang Anda gunakan?	GoPay OVO DANA Shopee Pay

			Other
8.		Apa yang paling sering Anda gunakan?	GoPay OVO DANA Shopee Pay Other
9.		Berapa kali anda menggunakan dalam seminggu?	Tidak pernah 2 kali 3-4 kali 5-6 kali Setiap hari
10.		Dari mana anda biasanya mendapatkan informasi tentang keamanan siber?	Media sosial Berita <i>online</i> Pelatihan formal Teman atau keluarga Lainnya Other
11.	Pernyataan untuk Menggali Variabel Dependen (<i>Knowledge</i>)	Verifikasi identitas pengirim diperlukan sebelum membuka <i>email</i> dari layanan .	1-4 (Sangat Tidak Setuju - Sangat Setuju)
12.		Menggunakan kata sandi yang kuat dan unik untuk setiap akun adalah penting.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
13.		Menggunakan jaringan WiFi publik untuk transaksi di tidak memiliki risiko keamanan.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
14.		Saya memahami konsep dan pentingnya autentikasi dua faktor (2FA).	1-4 (Sangat Tidak Paham - Sangat Paham)
15.		Saya tidak tahu tindakan apa yang harus diambil jika mengalami serangan siber pada akun .	1-4 (Sangat Tidak Setuju - Sangat Setuju)
16.		Saya tahu risiko keamanan yang terkait dengan penggunaan akun .	1-4 (Sangat Tidak Setuju - Sangat Setuju)
17.	Pernyataan untuk Menggali Variabel Dependen (<i>Attitude</i>)	Saya merasa penting untuk memverifikasi identitas pengirim sebelum membuka <i>email</i> dari layanan .	1-4 (Sangat Tidak Setuju - Sangat Setuju)
18.		Saya merasa bahwa kata sandi yang kuat dapat mengamankan akun saya.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
19.		Saya merasa nyaman menggunakan WiFi publik untuk transaksi di akun .	1-4 (Sangat Tidak Setuju - Sangat Setuju)

20.		Saya merasa bahwa penggunaan autentikasi dua faktor (2FA), untuk melindungi akun saya tidak diperlukan..	1-4 (Sangat Tidak Setuju - Sangat Setuju)
21.		Saya merasa perlu untuk selalu waspada terhadap kemungkinan serangan siber pada akun saya.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
22.		Saya merasa bahwa selalu aman digunakan tanpa langkah keamanan tambahan.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
23.	Pernyataan untuk Menggali Variabel Dependen <i>(Behavior)</i>	Saya terbiasa memverifikasi identitas pengirim sebelum membuka <i>email</i> dari layanan .	1-4 (Sangat Tidak Setuju - Sangat Setuju)
24.		Saya terbiasa menggunakan kata sandi yang sama untuk beberapa akun saya.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
25.		Saya terbiasa menghindari menggunakan WiFi publik untuk transaksi di .	1-4 (Sangat Tidak Setuju - Sangat Setuju)
26.		Saya terbiasa mengaktifkan dan menggunakan autentikasi dua faktor pada akun saya.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
27.		Saya terbiasa mengambil tindakan pencegahan setelah tahu tentang adanya serangan siber pada akun saya.	1-4 (Sangat Tidak Setuju - Sangat Setuju)
28.		Saya terbiasa memastikan keamanan aplikasi sebelum menggunakannya untuk transaksi.	1-4 (Sangat Tidak Setuju - Sangat Setuju)