



Department of Digital Business

Journal of Artificial Intelligence and Digital Business (RIGGS)

Homepage: <https://journal.ilmudata.co.id/index.php/RIGGS>

Vol. 1 No. 1 (2022) pp: 19449-19461

P-ISSN: 2963-9298, e-ISSN: 2963-914X

Kesadaran Risiko dan Strategi Mitigasi dalam Aplikasi Dompot Digital: Perspektif Masyarakat

Ahmad Nursodiq, Oki Herdiyanto, Muhammad Akhtar Hafiz Dwinov, Andi Ilham Nadjar Mustafa, Prima
Prayoga Putra

Fakultas Ilmu Komputer, Teknik Informatika, Universitas Pamulang

dosen02526@unpam.ac.id, okkyherdianto1@gmail.com, ilhamandi2704@gmail.com

Abstrak

Penelitian ini bertujuan menganalisis tingkat pemahaman masyarakat terhadap risiko keamanan dan strategi mitigasi dalam penggunaan aplikasi dompet digital pada aktivitas sehari-hari. Pertumbuhan transaksi nontunai menawarkan kemudahan, kecepatan, dan efisiensi, tetapi juga meningkatkan paparan terhadap phishing, penyalahgunaan kode OTP, kebocoran data pribadi, pengambilalihan akun, kesalahan transfer, serta kerugian akibat kelalaian pengguna. Penelitian menggunakan pendekatan kualitatif deskriptif dengan pengumpulan data melalui wawancara mendalam, observasi lapangan, dan dokumentasi. Kegiatan penelitian dilakukan di wilayah Tangerang Selatan dengan melibatkan informan yang aktif menggunakan GoPay, OVO, DANA, ShopeePay, dan LinkAja. Data dianalisis melalui tahapan reduksi data, penyajian data, serta penarikan dan verifikasi kesimpulan, sedangkan keabsahan temuan diperkuat melalui triangulasi sumber dan metode serta member checking. Hasil penelitian menunjukkan bahwa masyarakat telah mengenali risiko dasar, terutama penipuan yang meminta kode OTP dan tautan promosi palsu, tetapi pemahaman mengenai keamanan data, autentikasi berlapis, pengamanan perangkat, dan pengaturan privasi masih beragam. Strategi mitigasi yang paling sering diterapkan meliputi tidak membagikan PIN atau OTP, menggunakan kata sandi berbeda, memperbarui aplikasi, mengaktifkan verifikasi dua langkah, dan menghindari jaringan Wi-Fi publik. Namun, penerapan fitur keamanan lanjutan belum konsisten karena sebagian pengguna menganggapnya rumit. Temuan menegaskan perlunya edukasi keamanan digital yang berkelanjutan, peringatan aplikasi yang mudah dipahami, dan kolaborasi antara masyarakat, penyedia layanan, lembaga pendidikan, serta pemerintah untuk membangun transaksi dompet digital yang aman dan terpercaya.

Kata kunci: Dompot Digital, Risiko Keamanan, Mitigasi, Literasi Digital, Keamanan Transaksi

1. Latar Belakang

Perkembangan teknologi digital telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, termasuk dalam bidang keuangan. Salah satu inovasi yang berkembang pesat adalah penggunaan dompet digital (e-wallet) seperti DANA, OVO, GoPay, LinkAja, dan ShopeePay. Dompot digital menawarkan kemudahan dalam bertransaksi tanpa harus membawa uang tunai, cukup melalui ponsel yang terhubung dengan internet.

Berdasarkan laporan Bank Indonesia tahun 2024, jumlah transaksi digital di Indonesia terus meningkat hingga mencapai lebih dari 400 triliun rupiah per bulan, yang menunjukkan bahwa masyarakat semakin terbiasa menggunakan sistem pembayaran digital. Namun, di balik kemudahan tersebut terdapat risiko yang tidak bisa diabaikan, seperti penipuan online, kebocoran data pribadi, pencurian akun, hingga kesalahan transaksi. [1], [2]

Masih banyak pengguna yang belum memahami bagaimana cara melindungi akun mereka dari ancaman tersebut. Misalnya, beberapa pengguna masih membagikan kode OTP (One Time Password) kepada pihak yang tidak dikenal, menggunakan kata sandi yang mudah ditebak, atau tidak memperbarui aplikasi secara rutin. Kondisi ini menunjukkan pentingnya pemahaman masyarakat terhadap risiko dan strategi mitigasi dalam penggunaan aplikasi dompet digital agar transaksi tetap aman dan terhindar dari tindak kejahatan siber.

Oleh karena itu, penelitian ini dilakukan untuk mengetahui sejauh mana tingkat pemahaman masyarakat terhadap risiko penggunaan dompet digital, serta bagaimana strategi mitigasi yang telah dilakukan untuk menjaga keamanan transaksi digital dalam kehidupan sehari-hari.

Rumusan Masalah

Berdasarkan latar belakang yang ada, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Sejauh mana tingkat pemahaman masyarakat terhadap risiko penggunaan aplikasi dompet digital?
2. Apa saja bentuk risiko yang sering dihadapi masyarakat dalam penggunaan dompet digital?
3. Bagaimana strategi mitigasi yang dilakukan oleh masyarakat untuk mengurangi risiko penggunaan dompet digital?

Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengetahui tingkat pemahaman masyarakat terhadap risiko penggunaan aplikasi dompet digital.
2. Untuk mengidentifikasi berbagai risiko yang dihadapi masyarakat dalam transaksi menggunakan dompet digital.
3. Untuk mengetahui strategi mitigasi yang diterapkan oleh masyarakat guna menjaga keamanan dalam penggunaan dompet digital.

Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoretis: Menambah referensi dan wawasan akademik mengenai pemahaman risiko serta strategi mitigasi dalam penggunaan teknologi keuangan digital, khususnya dompet digital.
2. Manfaat Praktis: Memberikan informasi dan edukasi kepada masyarakat agar lebih berhati-hati dalam menggunakan aplikasi dompet digital serta memahami langkah-langkah keamanan yang tepat.
3. Manfaat bagi Peneliti Selanjutnya: Sebagai bahan acuan atau referensi bagi peneliti berikutnya yang ingin mengembangkan topik serupa dalam bidang keamanan siber dan perilaku pengguna teknologi finansial.

2. Metode Penelitian

Dompot digital atau e-wallet adalah aplikasi berbasis teknologi yang digunakan untuk menyimpan uang dalam bentuk saldo digital yang bisa digunakan untuk berbagai transaksi, seperti pembayaran tagihan, pembelian pulsa, transfer dana, hingga belanja online. Menurut Bank Indonesia (2023), dompet digital termasuk dalam kategori uang elektronik, yaitu alat pembayaran yang nilai uangnya disimpan secara elektronik pada suatu media server dan dikelola oleh penyelenggara resmi yang memiliki izin dari Bank Indonesia.

Beberapa contoh dompet digital yang populer di Indonesia antara lain GoPay, OVO, DANA, LinkAja, dan ShopeePay. Setiap platform memiliki kelebihan masing-masing, seperti promo cashback, kemudahan transfer, dan integrasi dengan layanan e-commerce.

Risiko dalam Penggunaan Dompot Digital

Meskipun dompet digital menawarkan kemudahan, terdapat beberapa risiko yang sering dihadapi pengguna. Menurut hasil riset dari Otoritas Jasa Keuangan (OJK, 2024), risiko-risiko tersebut meliputi: [1], [2]

Kebocoran Data Pribadi Terjadi ketika pengguna tidak berhati-hati dalam memberikan akses pada aplikasi pihak ketiga atau saat data dicuri oleh peretas (hacker).

Phishing dan Penipuan Online Modus ini biasanya melalui pesan atau tautan palsu yang meminta pengguna untuk memberikan informasi pribadi seperti PIN atau kode OTP.

Kesalahan Transaksi Contohnya salah transfer, salah memasukkan nominal, atau mengirim dana ke rekening yang tidak sesuai.

Keterbatasan Pengetahuan Pengguna Banyak pengguna belum memahami fitur keamanan seperti biometric lock, two-factor authentication, dan pengaturan batas transaksi.

Strategi Mitigasi Risiko Dompot Digital

Menurut Kementerian Komunikasi dan Informatika (2023), terdapat beberapa langkah mitigasi yang dapat dilakukan untuk meminimalkan risiko saat menggunakan dompet digital, antara lain: [1], [2]

Tidak Membagikan Kode OTP atau PIN kepada Siapa Pun. OTP bersifat rahasia dan hanya untuk digunakan oleh pemilik akun.

Mengaktifkan Verifikasi Ganda (Two-Factor Authentication). Fitur ini menambah lapisan keamanan sebelum transaksi dilakukan.

Memastikan Aplikasi Resmi dan Diperbarui Secara Berkala. Pembaruan biasanya mencakup peningkatan sistem keamanan dari celah siber terbaru.

Menghindari Penggunaan Wi-Fi Publik saat Bertransaksi. Jaringan publik rawan disusupi pihak yang ingin mencuri data pengguna.

Meningkatkan Literasi Digital. Dengan memahami risiko dan cara mengatasinya, pengguna bisa lebih waspada dan bijak dalam bertransaksi secara digital.

Penelitian Terdahulu

Beberapa penelitian sebelumnya yang relevan dengan topik ini antara lain:

Putri & Santoso (2023): Menemukan bahwa sebagian besar masyarakat menggunakan dompet digital karena faktor kepraktisan, namun masih minim pengetahuan tentang keamanan data pribadi. [3], [8]

Rachman (2022): Menunjukkan bahwa literasi digital memiliki hubungan yang signifikan terhadap tingkat keamanan transaksi online. [15]

Lestari (2024): Mengemukakan bahwa edukasi publik melalui media sosial efektif dalam meningkatkan kesadaran terhadap risiko dompet digital. [13]

Penelitian-penelitian tersebut menjadi dasar dalam penyusunan penelitian ini agar dapat memberikan gambaran yang lebih aktual tentang kondisi masyarakat di Tangerang Selatan.

3. Hasil dan Diskusi

Kerangka Pemikiran

Perkembangan teknologi finansial (fintech) telah memudahkan masyarakat dalam melakukan transaksi keuangan secara cepat dan praktis melalui berbagai aplikasi dompet digital seperti OVO, DANA, GoPay, LinkAja, dan ShopeePay. Namun, kemudahan ini juga menimbulkan berbagai risiko keamanan, seperti kebocoran data pribadi, penipuan digital, dan kesalahan transaksi akibat kurangnya pemahaman pengguna terhadap asyarakat keamanan digital.

Untuk itu, penting bagi masyarakat memiliki pemahaman yang baik tentang risiko dan mampu menerapkan strategi mitigasi yang tepat dalam penggunaan dompet digital.

Kerangka berpikir penelitian ini didasarkan pada hubungan logis antara tiga variabel utama berikut:

Penggunaan Dompot Digital (Variabel Awal)

Merupakan aktivitas masyarakat dalam memanfaatkan aplikasi keuangan digital untuk transaksi sehari-hari seperti pembayaran, pembelian, atau transfer dana.

Faktor pendorong: kemudahan, efisiensi waktu, promo, dan ketersediaan layanan online.

Namun, meningkatnya intensitas penggunaan dompet digital juga berpotensi meningkatkan risiko jika pengguna tidak memiliki pemahaman keamanan yang memadai.

Pemahaman Risiko (Variabel Antara)

Menunjukkan sejauh mana pengguna memahami potensi ancaman yang mungkin muncul, seperti:

1. Penipuan digital (phishing, link palsu, penipuan OTP).
2. Kebocoran data pribadi.
3. Penyalahgunaan akun.
4. Kesalahan dalam transaksi.

Pemahaman yang baik akan membantu pengguna bersikap lebih waspada dan mampu mengenali tanda-tanda risiko sejak dini.

Strategi Mitigasi (Variabel Akhir)

Adalah asya yang dilakukan asyarakat untuk mencegah atau mengurangi dampak risiko dari penggunaan dompet digital, seperti:

1. Mengaktifkan verifikasi dua langkah (2FA).
2. Tidak membagikan data pribadi atau kode OTP.
3. Memastikan aplikasi selalu diperbarui.
4. Menggunakan jaringan aman dan kata sandi kuat.

Tingkat pemahaman risiko yang baik diharapkan dapat mendorong penerapan strategi mitigasi yang efektif, sehingga masyarakat dapat bertransaksi secara aman dan nyaman.

Hubungan Antarvariabel

Hubungan logis dalam penelitian ini dapat dijelaskan sebagai berikut:

“Semakin tinggi tingkat pemahaman masyarakat terhadap risiko penggunaan dompet digital, maka semakin baik pula strategi mitigasi yang dilakukan dalam menjaga keamanan transaksi digital”.

Gambar 1. Kerangka Pemikiran

**PENGUNAAN DOMPET DIGITAL → TINGKAT PEMAHAMAN RISIKO → STRATEGI MITIGASI
PENGUNA → TINGKAT KEAMANAN TRANSAKSI DIGITAL**

Tabel 1. Hubungan Penggunaan Dompot Digital, Pemahaman Risiko, Mitigasi, dan Keamanan Transaksi

No	Variabel	Keterangan Hubungan
1	Penggunaan Dompot Digital	Meningkatnya penggunaan aplikasi transaksi digital
2	Pemahaman Risiko	Mempengaruhi kesadaran pengguna dalam menjaga keamanan

3	Strategi Mitigasi	Diterapkan untuk mencegah atau mengurangi risiko transaksi
4	Keamanan Transaksi	Hasil akhir dari penerapan mitigasi dan pemahaman pengguna

Jenis Penelitian

Penelitian ini menggunakan metode kualitatif deskriptif, yaitu penelitian yang berfokus pada pengumpulan data melalui wawancara dan observasi lapangan untuk menggambarkan pemahaman masyarakat terhadap risiko dan strategi mitigasi dalam penggunaan aplikasi dompet digital.

Metode ini dipilih karena dapat menggambarkan secara mendalam pandangan, pengalaman, dan perilaku pengguna dompet digital dalam kehidupan sehari-hari di wilayah Tangerang Selatan.

Lokasi dan Waktu Penelitian

Lokasi Penelitian: Kota Tangerang Selatan, Provinsi Banten. Lokasi ini dipilih karena merupakan salah satu kota dengan tingkat penggunaan layanan digital dan dompet elektronik yang tinggi di wilayah Jabodetabek.

Waktu Penelitian: Penelitian dilaksanakan pada bulan September - Oktober 2025, meliputi tahap persiapan, pengumpulan data, analisis data, dan penyusunan laporan.

Subjek dan Objek Penelitian

Subjek Penelitian: Masyarakat pengguna dompet digital yang berdomisili di Tangerang Selatan, meliputi pelajar, mahasiswa, pegawai, dan pelaku UMKM.

Objek Penelitian: Pemahaman masyarakat terhadap risiko dan strategi mitigasi dalam penggunaan aplikasi dompet digital.

Teknik Pengumpulan Data

Data dikumpulkan melalui beberapa teknik berikut:

Wawancara Mendalam (In-depth Interview) Dilakukan kepada 10 responden pengguna dompet digital di wilayah Tangerang Selatan dengan tujuan mengetahui tingkat pemahaman dan pengalaman mereka terkait risiko dan keamanan transaksi digital.

Observasi Lapangan Peneliti melakukan pengamatan langsung terhadap perilaku masyarakat dalam menggunakan dompet digital saat bertransaksi, seperti di warung kopi, toko retail, dan UMKM lokal.

Dokumentasi Mengumpulkan data dari literatur, berita resmi, laporan Bank Indonesia, dan artikel ilmiah terkait keamanan dompet digital.

Teknik Analisis Data

Penelitian ini menggunakan model analisis Miles dan Huberman (1994), yang terdiri dari tiga tahapan utama:

Reduksi Data (Data Reduction): Menyeleksi dan menyederhanakan hasil wawancara dan observasi agar fokus pada hal-hal yang relevan dengan tujuan penelitian.

Penyajian Data (Data Display): Menyusun data ke dalam bentuk narasi, tabel, dan kutipan wawancara agar mudah dipahami dan dianalisis.

Penarikan Kesimpulan (Conclusion Drawing): Menarik kesimpulan berdasarkan pola dan makna dari hasil temuan di lapangan.

Keabsahan Data

Untuk memastikan data yang diperoleh valid dan dapat dipercaya, digunakan teknik triangulasi sumber dan metode, yaitu dengan membandingkan hasil wawancara dengan data observasi dan literatur pendukung.

Selain itu, peneliti juga melakukan member checking, yaitu meminta konfirmasi dari responden mengenai hasil interpretasi data agar tidak terjadi kesalahpahaman. Langkah-langkah Penelitian

Berikut tahapan penelitian yang dilakukan:

1. Menentukan topik dan rumusan masalah.
2. Mengumpulkan teori dan referensi terkait dompet digital serta risiko keamanannya.
3. Menyusun instrumen wawancara dan pedoman observasi.
4. Melakukan wawancara dan observasi lapangan.
5. Mengolah dan menganalisis data hasil penelitian.
6. Menyusun laporan penelitian lengkap.

Gambaran Umum Lokasi Penelitian

Penelitian ini dilakukan di Kota Tangerang Selatan, Provinsi Banten. Tangerang Selatan dikenal sebagai salah satu kota dengan tingkat literasi digital yang cukup tinggi, terutama di kalangan anak muda, mahasiswa, dan pelaku usaha mikro.

Banyak transaksi harian, seperti pembayaran di kafe, toko, dan transportasi online, yang sudah menggunakan dompet digital seperti DANA, OVO, GoPay, dan ShopeePay.

Kondisi inilah yang membuat Tangerang Selatan menjadi lokasi yang relevan untuk meneliti bagaimana masyarakat memahami risiko dan strategi mitigasi dalam menggunakan dompet digital.

Profil Responden

Dalam penelitian ini, kami mewawancarai 4 orang responden yang merupakan pengguna aktif dompet digital.

Tabel 2. Profil Responden

No	Inisial	Usia	Pekerjaan	Dompot Digital yang Digunakan	Lama Penggunaan
1	AN	22	Mahasiswa	DANA, GoPay	3 Tahun
2	RS	27	Pegawai Swasta	OVO	4 Tahun
3	IL	31	Pelaku UMKM	ShopeePay	2 Tahun
4	KT	24	Freelancer	DANA, LinkAja	3 Tahun

Hasil Wawancara

Dari Hasil wawancara dengan responden, kami memperoleh beberapa temuan yang menarik sebagai berikut:

Tingkat Pemahaman terhadap Risiko

Sebagian besar responden mengetahui adanya risiko dalam penggunaan dompet digital, namun tingkat pemahaman mereka masih beragam. Beberapa contoh kutipan responden:

“Saya tahu sih bisa kena penipuan, makanya sekarang nggak pernah kasih kode OTP ke siapa pun.” (AN, Mahasiswa)

“Saya baru tahu kalau link promo palsu bisa nyuri data, jadi sekarang lebih hati-hati.” (IL, Pelaku UMKM)

Namun, masih ada responden yang belum sepenuhnya sadar risiko digital, terutama dalam hal keamanan data pribadi dan kebiasaan menyimpan PIN di catatan ponsel.

Bentuk Risiko yang Dihadapi

Beberapa risiko nyata yang dialami atau diketahui oleh responden antara lain:

Pesan phishing dari akun palsu yang mengatasnamakan penyedia layanan.

Kesalahan transfer ke nomor lain.

Aplikasi mendadak terblokir karena login di perangkat berbeda.

Meski sebagian besar belum pernah mengalami kerugian finansial, hampir semua responden pernah menerima pesan mencurigakan terkait dompet digital mereka.

Strategi Mitigasi yang Dilakukan

Bentuk upaya mitigasi yang dilakukan masyarakat cukup beragam, di antaranya:

Tidak memberikan kode OTP atau PIN kepada siapa pun.

Menggunakan kata sandi yang berbeda untuk setiap aplikasi.

Mengaktifkan verifikasi dua langkah (2FA).

Mengupdate aplikasi secara rutin.

Tidak melakukan transaksi di jaringan Wi-Fi publik.

Sebagian responden juga mengaku mendapatkan informasi keamanan dari media sosial atau kampanye digital dari aplikasi dompet digital itu sendiri.

Observasi Lapangan

Selama observasi di beberapa lokasi seperti kafe, minimarket, dan area kampus, ditemukan bahwa:

Penggunaan dompet digital sudah menjadi kebiasaan umum.

Banyak pengguna yang langsung membuka aplikasi tanpa memperhatikan pop-up keamanan.

Beberapa pelaku UMKM sudah mulai mewaspadai penipuan, namun belum memahami fitur keamanan lanjutan seperti biometric lock atau PIN transaksi tambahan.

Hal ini menunjukkan bahwa masyarakat sudah melek digital secara praktis, tetapi masih perlu edukasi keamanan digital secara mendalam.

Pembahasan

Hasil penelitian menunjukkan bahwa tingkat pemahaman masyarakat terhadap risiko penggunaan dompet digital masih berada pada tingkat menengah. Masyarakat tahu bahwa dompet digital memiliki potensi risiko, namun belum semuanya memahami bagaimana cara kerja sistem keamanan digital secara detail. [3], [4], [13]

Temuan ini sejalan dengan penelitian Putri & Santoso (2023) yang menyebutkan bahwa sebagian besar pengguna e-wallet hanya fokus pada kemudahan dan promo, bukan pada aspek keamanan.

Dari sisi mitigasi, masyarakat di Tangerang Selatan menunjukkan perilaku yang cukup positif dengan tidak mudah percaya pada pesan mencurigakan dan mulai menerapkan langkah keamanan dasar. Namun, literasi keamanan digital masih perlu ditingkatkan, terutama dalam hal pembuatan kata sandi kuat, pengaturan privasi, dan verifikasi akun. [1], [2], [15]

Kesenjangan antara Kesadaran Umum dan Pemahaman Teknis

Pemahaman risiko yang ditemukan dalam penelitian ini memperlihatkan adanya perbedaan antara kesadaran umum dan kemampuan teknis. Pengguna sudah mengenali bahwa penipuan, kebocoran data, dan kesalahan transaksi dapat terjadi, tetapi pengetahuan tersebut belum selalu diterjemahkan menjadi pemahaman tentang bagaimana ancaman bekerja. Seseorang dapat mengetahui bahwa kode OTP tidak boleh dibagikan, namun belum tentu memahami bahwa penipu dapat membangun situasi mendesak, menyamar sebagai petugas resmi, atau mengarahkan korban ke halaman tiruan yang tampak sah. Kesenjangan ini penting karena keamanan transaksi tidak hanya ditentukan oleh keberadaan fitur teknologi, melainkan juga oleh kemampuan pengguna membaca konteks, memeriksa sumber pesan, dan menunda tindakan ketika terdapat tanda yang mencurigakan. Studi mengenai penggunaan e-wallet di Indonesia juga menempatkan keamanan, privasi, dan kepercayaan sebagai unsur penting yang memengaruhi perilaku pengguna [3], [4].

Temuan observasi bahwa pengguna sering langsung membuka aplikasi tanpa membaca peringatan menunjukkan dominannya kebiasaan praktis dibandingkan evaluasi risiko. Perilaku ini dapat muncul karena transaksi digital telah menjadi rutinitas yang dilakukan dengan cepat. Ketika penggunaan menjadi otomatis, perhatian pengguna terhadap pesan keamanan cenderung menurun, terutama jika tampilan peringatan dianggap berulang atau tidak relevan. Kondisi tersebut tidak berarti pengguna tidak peduli terhadap keamanan, tetapi menunjukkan bahwa pesan keamanan perlu dirancang secara kontekstual, ringkas, dan muncul pada saat keputusan berisiko akan dilakukan. Penelitian tentang keberlanjutan penggunaan e-wallet menegaskan bahwa kualitas informasi keamanan, perlindungan privasi, enkripsi, dan proses transaksi membentuk persepsi keamanan serta kepuasan pengguna [13]. Dengan demikian, peningkatan pemahaman perlu diarahkan pada keterampilan praktis, bukan hanya penyampaian larangan umum.

Phishing, Rekayasa Sosial, dan Penyalahgunaan OTP

Risiko yang paling mudah dikenali oleh responden adalah pesan phishing dan permintaan kode OTP. Temuan tersebut konsisten dengan karakter serangan terhadap layanan pembayaran digital yang lebih banyak mengeksploitasi manusia daripada menembus sistem inti penyedia. Pelaku biasanya memanfaatkan rasa takut, ketegesaan, iming-iming hadiah, atau klaim adanya masalah akun agar pengguna segera mengikuti instruksi. Dalam keadaan tertekan, pengguna dapat mengabaikan alamat pengirim, mengklik tautan palsu, atau memberikan informasi rahasia. Oleh karena itu, perlindungan yang efektif perlu menggabungkan edukasi tentang pola rekayasa sosial dengan mekanisme teknis yang membatasi dampak ketika pengguna melakukan kesalahan. Aturan keamanan sistem pembayaran Bank Indonesia menekankan identifikasi risiko, proteksi data, deteksi serangan, respons insiden, dan pemulihan sebagai rangkaian yang saling berhubungan [1], [2].

Larangan membagikan OTP harus dijelaskan sebagai bagian dari pengamanan identitas dan otorisasi transaksi. OTP bukan sekadar angka sementara, tetapi bukti bahwa pemilik perangkat menyetujui proses tertentu. Pengguna perlu memahami bahwa petugas resmi tidak memerlukan OTP, PIN, atau kata sandi untuk melakukan verifikasi layanan. Edukasi juga harus membedakan pesan promosi resmi, notifikasi transaksi, dan komunikasi mencurigakan. Pengguna sebaiknya diarahkan untuk membuka aplikasi melalui ikon resmi, tidak melalui tautan dalam pesan, serta menghubungi pusat bantuan dari kanal yang tercantum di aplikasi. Penelitian tentang autentikasi berbasis identitas perangkat menunjukkan pentingnya pengikatan akun dengan perangkat, verifikasi identitas, dan kontrol akses untuk memperkuat keamanan aplikasi pembayaran [7]. Praktik tersebut akan lebih efektif apabila pengguna memperoleh penjelasan sederhana mengenai alasan setiap langkah keamanan.

Kebocoran Data Pribadi dan Pengambilalihan Akun

Kebocoran data pribadi merupakan risiko yang lebih sulit diamati dibandingkan kesalahan transfer atau pesan penipuan. Pengguna mungkin tidak langsung mengetahui bahwa nomor telepon, alamat surat elektronik, riwayat transaksi, atau informasi identitas telah diketahui pihak lain. Data tersebut dapat dikombinasikan untuk menyusun pesan yang tampak meyakinkan, menjawab pertanyaan pemulihan akun, atau melakukan percobaan pengambilalihan akun. Karena itu, mitigasi tidak cukup hanya dengan merahasiakan OTP. Pengguna perlu membatasi izin aplikasi, menghindari penggunaan kata sandi yang sama, mengaktifkan kunci layar dan biometrik, serta memeriksa perangkat yang terhubung. Persepsi mengenai keamanan data pribadi terbukti berhubungan positif dengan keputusan menggunakan e-wallet, terutama pada pengguna UMKM yang menjadikan dompet digital sebagai bagian dari kegiatan usaha [8].

Pengelolaan data oleh penyedia layanan juga menentukan tingkat kepercayaan. Pengguna membutuhkan informasi yang jelas tentang data apa yang dikumpulkan, tujuan pemrosesan, lama penyimpanan, dan cara mengajukan pengaduan ketika terjadi dugaan penyalahgunaan. Informasi tersebut sebaiknya tidak hanya ditempatkan dalam kebijakan privasi yang panjang, tetapi diterjemahkan menjadi pilihan yang mudah dipahami di dalam aplikasi. Temuan penelitian ini mengenai keterbatasan pemahaman pengaturan privasi menunjukkan bahwa transparansi harus diikuti dengan desain yang membantu pengguna membuat keputusan. Kajian mengenai keamanan dompet digital menekankan bahwa ancaman dapat muncul pada lapisan perangkat, aplikasi, autentikasi, penyimpanan kredensial, dan proses pemulihan [10]. Walaupun konteks teknologi dompet dapat berbeda, prinsip pertahanan berlapis tetap relevan untuk mengurangi ketergantungan pada satu mekanisme keamanan.

Kesalahan Transaksi dan Keamanan Operasional Pengguna

Kesalahan transfer yang disebutkan oleh responden menunjukkan bahwa risiko dompet digital tidak selalu berasal dari tindakan kriminal. Antarmuka yang cepat, daftar penerima yang mirip, kebiasaan menyalin nomor, atau kurangnya pemeriksaan nominal dapat menimbulkan kerugian. Risiko operasional semacam ini perlu dipahami sebagai bagian dari keamanan penggunaan. Strategi mitigasinya mencakup pemeriksaan nama penerima,

konfirmasi nominal, penggunaan daftar favorit yang telah diverifikasi, dan penghindaran transaksi ketika perhatian pengguna terbagi. Penyedia layanan dapat membantu melalui tampilan konfirmasi yang menonjolkan identitas penerima, jeda singkat sebelum transaksi bernilai besar, serta notifikasi yang memungkinkan pengguna segera melaporkan kesalahan. Kemudahan penggunaan memang menjadi pendorong adopsi e-wallet, tetapi kemudahan harus tetap disertai kontrol yang mencegah tindakan tidak disengaja [9], [11].

Keamanan operasional juga mencakup pengelolaan perangkat. Ponsel yang tidak memiliki kunci layar, sistem operasi yang tidak diperbarui, atau aplikasi yang dipasang dari sumber tidak resmi meningkatkan kemungkinan penyalahgunaan. Pembaruan aplikasi yang telah dilakukan sebagian responden merupakan langkah positif karena perbaikan keamanan sering disertakan dalam versi terbaru. Namun, pembaruan perlu dilengkapi dengan kebiasaan meninjau izin aplikasi, menghapus aplikasi yang tidak digunakan, dan mengaktifkan fitur pencarian atau penghapusan perangkat dari jarak jauh. Pengguna juga perlu memiliki prosedur ketika ponsel hilang, misalnya segera memblokir kartu SIM, mengganti kata sandi, dan menghubungi penyedia e-wallet. Pendekatan ini selaras dengan gagasan bahwa keamanan pembayaran digital dibentuk oleh interaksi antara teknologi, prosedur, dan perilaku pengguna, bukan oleh satu fitur tunggal [5], [12].

Perbedaan Usia, Pengalaman Digital, dan Literasi Keamanan

Perbedaan tingkat pemahaman antara pengguna yang lebih muda dan pengguna berusia di atas 30 tahun perlu ditafsirkan secara hati-hati. Usia tidak selalu identik dengan kemampuan digital, tetapi pengalaman menggunakan aplikasi, frekuensi memperoleh informasi, dan kesempatan belajar dapat membentuk kepercayaan diri pengguna. Kelompok muda cenderung lebih sering berinteraksi dengan aplikasi dan media sosial sehingga lebih cepat mengenali pola pesan palsu. Namun, kebiasaan tinggi juga dapat memunculkan rasa terlalu percaya diri dan mengurangi kehati-hatian. Sebaliknya, pengguna yang lebih jarang menggunakan teknologi mungkin lebih berhati-hati, tetapi mengalami kesulitan memahami istilah teknis atau mengatur fitur keamanan. Penelitian mengenai adopsi e-wallet menunjukkan bahwa literasi keuangan digital, persepsi keamanan, kemudahan, dan pengaruh sosial berperan dalam pembentukan niat penggunaan [15].

Program edukasi karena itu perlu disesuaikan dengan profil pengguna. Materi untuk pengguna pemula dapat menggunakan simulasi sederhana tentang pesan palsu, cara memeriksa tautan, dan langkah pengaduan. Pengguna yang lebih berpengalaman dapat diberikan materi tentang pengaturan privasi, autentikasi berlapis, manajemen kata sandi, dan pemantauan aktivitas akun. Pelaku UMKM memerlukan tambahan panduan mengenai pemisahan akun pribadi dan usaha, pengelolaan perangkat kasir, serta pencatatan transaksi. Pendekatan berjenjang membantu menghindari dua masalah: materi yang terlalu umum bagi pengguna mahir dan materi yang terlalu teknis bagi pengguna pemula. Studi lintas kelompok pengguna di Indonesia menunjukkan bahwa faktor kepercayaan, kemudahan, dan kesesuaian gaya hidup dapat bekerja secara berbeda menurut karakteristik demografis [16].

Evaluasi Strategi Mitigasi yang Telah Diterapkan

Strategi mitigasi yang dilakukan responden, seperti tidak memberikan OTP, menggunakan kata sandi berbeda, memperbarui aplikasi, mengaktifkan verifikasi dua langkah, dan menghindari Wi-Fi publik, menunjukkan fondasi perilaku keamanan yang cukup baik. Kekuatan utama strategi tersebut adalah sifatnya yang langsung dapat dilakukan oleh pengguna tanpa memerlukan perangkat khusus. Namun, efektivitasnya bergantung pada konsistensi. Pengguna yang mengaktifkan verifikasi ganda tetapi masih menggunakan PIN yang mudah ditebak tetap memiliki celah. Demikian pula, menghindari Wi-Fi publik tidak cukup jika pengguna memasang aplikasi dari sumber tidak resmi atau memberikan izin akses berlebihan. Karena itu, mitigasi sebaiknya dipahami sebagai paket kebiasaan yang saling memperkuat. Penelitian tentang niat menggunakan e-wallet menempatkan kepercayaan dan keamanan sebagai faktor penting bersama kemudahan penggunaan [4].

Anggapan bahwa fitur keamanan lanjutan terasa “ribet” menunjukkan adanya pertukaran antara kenyamanan dan perlindungan. Pengguna cenderung menonaktifkan fitur apabila langkah tambahan muncul terlalu sering, tidak dijelaskan manfaatnya, atau menghambat transaksi kecil. Penyedia layanan perlu menerapkan keamanan adaptif, yaitu tingkat verifikasi yang menyesuaikan konteks transaksi, perangkat, lokasi, dan pola penggunaan. Transaksi rutin bernilai kecil dapat memperoleh alur sederhana, sedangkan login dari perangkat baru atau transaksi tidak biasa memerlukan verifikasi tambahan. Pendekatan tersebut membuat keamanan lebih proporsional dan mengurangi kelelahan pengguna. Penelitian tentang dampak keamanan terhadap adopsi dompet seluler menunjukkan bahwa keamanan memengaruhi kepercayaan dan sikap, yang selanjutnya membentuk niat penggunaan [14]. Dengan demikian, desain keamanan harus menjaga keseimbangan antara perlindungan dan pengalaman pengguna.

Autentikasi Berlapis, Kata Sandi, dan Perlindungan Perangkat

Autentikasi berlapis perlu ditempatkan sebagai standar, bukan pilihan tambahan yang hanya digunakan setelah terjadi insiden. Kombinasi PIN, biometrik, identitas perangkat, dan kode verifikasi membuat penyerang harus melewati lebih dari satu penghalang. Akan tetapi, setiap lapisan harus dirancang agar dapat dipulihkan dengan aman. Proses pemulihan akun yang terlalu mudah dapat dimanfaatkan pelaku, sedangkan proses yang terlalu rumit dapat merugikan pengguna sah. Penyedia perlu memastikan bahwa perubahan nomor telepon, pergantian perangkat, dan pemulihan akses disertai verifikasi identitas yang memadai serta notifikasi ke kanal lama. Kerangka autentikasi berbasis identitas perangkat menawarkan contoh bagaimana pengenalan perangkat dapat memperkecil peluang akses tidak sah [7].

Manajemen kata sandi juga perlu dijelaskan secara praktis. Anjuran menggunakan kata sandi kuat tidak efektif apabila pengguna tidak mengetahui cara membuat dan menyimpannya. Pengguna dapat diarahkan memakai frasa sandi yang panjang, berbeda untuk setiap layanan, dan tidak disimpan dalam catatan terbuka. Penggunaan pengelola kata sandi tepercaya dapat dipertimbangkan bagi pengguna yang memiliki banyak akun. Biometrik memberi kenyamanan, tetapi tetap perlu dilindungi oleh PIN perangkat dan mekanisme penguncian setelah beberapa percobaan gagal. Pengamanan perangkat, aplikasi, dan akun harus dipandang sebagai satu kesatuan. Regulasi keamanan siber Bank Indonesia juga menekankan tata kelola, pencegahan, deteksi, respons, dan pemulihan sebagai siklus berkelanjutan [1], [2], sehingga desain keamanan tidak berhenti pada autentikasi awal.

Peran Penyedia Layanan dan Desain Peringatan Keamanan

Hasil observasi tentang diabaikannya pop-up keamanan memperlihatkan bahwa penyedia layanan perlu mengevaluasi cara menyampaikan peringatan. Peringatan yang terlalu sering, panjang, atau menggunakan istilah teknis berpotensi dilewati tanpa dibaca. Pesan sebaiknya menjelaskan risiko, tindakan yang harus dilakukan, dan konsekuensi secara singkat. Pada saat pengguna akan mengirim dana ke penerima baru, aplikasi dapat menampilkan pertanyaan verifikasi yang relevan, misalnya memastikan pengguna tidak sedang diarahkan pihak lain atau diminta membagikan OTP. Peringatan yang kontekstual lebih efektif daripada pesan umum yang selalu sama. Faktor informasi keamanan dan proses transaksi terbukti membentuk persepsi keamanan dan kepuasan pengguna e-wallet di Indonesia [13].

Selain peringatan, penyedia perlu menyediakan mekanisme pelaporan yang cepat. Pengguna yang menerima pesan phishing atau melihat transaksi mencurigakan harus dapat mengakses tombol bantuan tanpa mencari informasi di luar aplikasi. Pelaporan perlu menghasilkan nomor tiket, petunjuk tindakan darurat, dan pembaruan status yang transparan. Penyedia juga dapat menggunakan data laporan untuk memperbarui daftar pola penipuan, memblokir akun penerima yang mencurigakan, dan mengirimkan edukasi kepada kelompok pengguna yang relevan. Penguatan keamanan semacam ini mendukung kepercayaan jangka panjang. Kajian adopsi e-wallet di Indonesia menunjukkan bahwa *perceived trust* berpengaruh terhadap niat dan penggunaan aktual [16]. Oleh sebab itu, respons terhadap insiden harus dipandang sebagai bagian dari kualitas layanan, bukan hanya fungsi teknis di belakang layar.

Peran Pendidikan, Pemerintah, dan Kolaborasi Ekosistem

Keamanan dompet digital tidak dapat dibebankan sepenuhnya kepada pengguna. Lembaga pendidikan, pemerintah, penyedia layanan, perbankan, operator telekomunikasi, dan pelaku usaha memiliki peran yang saling melengkapi. Institusi pendidikan dapat memasukkan keamanan transaksi digital ke dalam kegiatan literasi, orientasi mahasiswa, atau pelatihan masyarakat. Materi sebaiknya berbasis kasus yang dekat dengan pengalaman sehari-hari, seperti undangan hadiah, perubahan nomor layanan pelanggan, dan permintaan pembayaran melalui akun pribadi. Pemerintah dan regulator dapat memperkuat standar penanganan insiden, perlindungan data, serta mekanisme koordinasi antarpelaku. Kebijakan Bank Indonesia tahun 2024 memberikan kerangka yang menekankan kesiapan penyelenggara menghadapi risiko dan insiden siber [1], [2].

Kolaborasi juga diperlukan karena pelaku penipuan sering berpindah kanal dari media sosial, telepon, pesan instan, rekening bank, hingga e-wallet. Informasi mengenai akun, nomor, atau pola serangan perlu dibagikan melalui mekanisme yang mematuhi perlindungan data. Kampanye publik dapat menggunakan pesan yang konsisten agar pengguna tidak menerima instruksi yang bertentangan. Bagi masyarakat, keberadaan satu kanal resmi untuk memeriksa informasi dan melaporkan insiden akan mengurangi kebingungan. Penguatan literasi finansial digital terbukti relevan terhadap niat menggunakan e-wallet dan kemampuan mengevaluasi keamanan layanan [15]. Kolaborasi ekosistem pada akhirnya bertujuan membentuk budaya keamanan, yaitu kebiasaan memeriksa, mengonfirmasi, dan melaporkan, bukan hanya reaksi sementara setelah terjadi kerugian.

Implikasi bagi Pelaku UMKM dan Transaksi Harian

Pelaku UMKM dalam penelitian ini menunjukkan penggunaan dompet digital sebagai bagian dari aktivitas usaha, tetapi belum seluruhnya memahami fitur keamanan lanjutan. Bagi UMKM, insiden keamanan dapat berdampak lebih luas karena satu akun dapat menerima banyak pembayaran, menyimpan riwayat pelanggan, dan menjadi sumber pencatatan kas. Mitigasi perlu mencakup pemisahan perangkat atau profil kerja, pembatasan akses bagi pegawai, rekonsiliasi transaksi harian, dan pencadangan bukti pembayaran. Pemilik usaha juga harus membedakan notifikasi asli dengan tangkapan layar yang dapat dimanipulasi. Penelitian pada UMKM di Jakarta menemukan bahwa literasi digital dan persepsi keamanan data pribadi berpengaruh positif terhadap keputusan menggunakan e-wallet sebagai sistem pembayaran [8].

Pada transaksi harian, pengguna dan pedagang dapat menerapkan kebiasaan verifikasi sederhana tanpa memperlambat pelayanan. Pedagang memeriksa notifikasi pada aplikasi atau sistem kasir, bukan hanya bukti dari pelanggan. Pengguna memastikan nama merchant dan nominal sebelum menyetujui pembayaran. Apabila perangkat digunakan bersama, akses ke aplikasi keuangan tidak boleh dibiarkan terbuka. Penyedia e-wallet dapat mendukung UMKM melalui dashboard transaksi, pengaturan pengguna, notifikasi anomali, dan materi edukasi khusus. Penetrasi e-wallet berpotensi mendukung inklusi keuangan, tetapi manfaat tersebut perlu disertai kesiapan keamanan dan kemampuan operasional [6]. Dengan demikian, perlindungan UMKM bukan hanya soal mencegah kehilangan saldo, tetapi juga menjaga kelangsungan usaha dan kepercayaan pelanggan.

Sintesis Temuan dengan Perilaku Adopsi Dompet Digital

Temuan penelitian memperlihatkan bahwa masyarakat tetap menggunakan dompet digital meskipun menyadari adanya risiko. Hal ini menunjukkan bahwa keputusan penggunaan merupakan hasil penilaian antara manfaat, kemudahan, kepercayaan, dan risiko. Manfaat transaksi cepat dan integrasi dengan kebutuhan sehari-hari dapat lebih dominan daripada kekhawatiran, terutama ketika pengguna belum pernah mengalami kerugian. Kondisi ini menjelaskan mengapa kesadaran risiko tidak otomatis menghasilkan perilaku mitigasi yang lengkap. Model adopsi teknologi pada penelitian terdahulu menunjukkan bahwa ekspektasi kinerja, kemudahan, pengaruh sosial, kondisi pendukung, kepercayaan, dan keamanan bersama-sama membentuk niat serta penggunaan [11], [16].

Dalam perspektif tersebut, strategi keamanan yang efektif tidak seharusnya mengurangi manfaat utama dompet digital. Edukasi harus membantu pengguna mempertahankan kemudahan sambil membangun kebiasaan aman. Penyedia layanan perlu menjadikan keamanan sebagai bagian dari nilai produk, misalnya melalui notifikasi yang informatif, pemulihan akun yang jelas, dan perlindungan transaksi yang terlihat. Kepercayaan tumbuh ketika pengguna memahami apa yang dilakukan sistem dan mengetahui cara memperoleh bantuan. Penelitian mengenai faktor keamanan informasi menunjukkan bahwa persepsi keamanan dapat memengaruhi konfirmasi harapan, kepuasan, dan niat melanjutkan penggunaan [13]. Karena itu, keamanan bukan hambatan adopsi, melainkan fondasi keberlanjutan penggunaan jika dirancang dan dikomunikasikan dengan baik.

Implikasi Metodologis dan Keterbatasan Interpretasi

Pendekatan kualitatif memberikan ruang untuk memahami pengalaman, alasan, dan kebiasaan pengguna yang tidak selalu terlihat melalui angka. Kutipan responden memperlihatkan bagaimana pengalaman menerima pesan mencurigakan dapat mengubah perilaku, sedangkan observasi menunjukkan adanya perbedaan antara pengetahuan yang diucapkan dan tindakan saat bertransaksi. Kekuatan tersebut perlu dipertahankan dalam penelitian lanjutan melalui dokumentasi konteks wawancara, karakteristik penggunaan, dan jenis insiden yang pernah dialami. Triangulasi sumber dan metode membantu mengurangi ketergantungan pada satu jenis data, terutama karena responden dapat menyampaikan jawaban yang dianggap aman secara sosial meskipun perilaku aktualnya berbeda.

Interpretasi temuan tetap perlu mempertimbangkan keterbatasan jumlah dan cakupan informan serta fokus lokasi penelitian. Hasil tidak dimaksudkan untuk mewakili seluruh pengguna dompet digital di Indonesia, melainkan menggambarkan pola pemahaman dan mitigasi pada konteks yang diteliti. Penelitian berikutnya dapat membandingkan kelompok usia, pekerjaan, tingkat literasi, dan pengalaman insiden; menggabungkan observasi dengan survei; serta menguji efektivitas intervensi edukasi sebelum dan sesudah pelatihan. Kajian keamanan dan adopsi yang lebih luas menunjukkan bahwa karakter pengguna dan konteks penggunaan dapat memengaruhi hubungan antara keamanan, kepercayaan, dan niat penggunaan [14], [15]. Pengembangan tersebut akan memperkuat dasar penyusunan program literasi dan desain layanan yang lebih tepat sasaran.

Arah Strategi Mitigasi yang Terintegrasi

Berdasarkan keseluruhan temuan, strategi mitigasi dapat disusun dalam tiga lapisan. Lapisan pertama adalah kebiasaan pengguna, meliputi perlindungan OTP dan PIN, pemeriksaan penerima, penggunaan kata sandi berbeda,

pembaruan aplikasi, serta penghindaran tautan dan jaringan yang tidak terpercaya. Lapisan kedua adalah kontrol penyedia, meliputi autentikasi adaptif, deteksi anomali, pembatasan transaksi, notifikasi kontekstual, dan proses pemulihan yang aman. Lapisan ketiga adalah dukungan ekosistem melalui regulasi, pertukaran informasi, edukasi, dan penanganan pengaduan. Ketiga lapisan harus berjalan bersama karena kelemahan pada satu lapisan dapat dikompensasi oleh lapisan lain. Prinsip pertahanan berlapis tersebut selaras dengan kerangka pengelolaan keamanan dan ketahanan siber pada sistem pembayaran [1], [2].

Penerapan strategi terintegrasi juga perlu dievaluasi secara berkala. Pola penipuan berubah mengikuti kebiasaan pengguna dan fitur baru aplikasi. Edukasi yang efektif pada satu periode dapat menjadi kurang relevan ketika pelaku menggunakan modus baru. Penyedia layanan dan lembaga terkait perlu memantau laporan, menguji pemahaman pengguna, serta memperbarui skenario komunikasi. Bagi masyarakat, indikator keberhasilan bukan hanya tidak mengalami kerugian, tetapi juga mampu mengenali ancaman, menghentikan proses mencurigakan, dan melaporkannya melalui kanal resmi. Dengan pendekatan tersebut, penggunaan dompet digital dapat tetap berkembang tanpa mengabaikan perlindungan data dan keamanan transaksi. Keamanan yang konsisten akan memperkuat kepercayaan dan mendukung keberlanjutan adopsi layanan pembayaran digital [3], [13], [16].

Temuan Utama Penelitian

Mayoritas pengguna sudah menyadari risiko dasar seperti penipuan OTP.

Sebagian masih mengabaikan keamanan akun karena merasa aman selama tidak ada masalah.

Edukasi keamanan dari pihak penyedia aplikasi terbukti membantu meningkatkan kesadaran pengguna.

Penggunaan fitur verifikasi ganda masih belum maksimal karena sebagian pengguna merasa “ribet”.

4. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan mengenai “Pemahaman Masyarakat terhadap Risiko dan Strategi Mitigasi Penggunaan Aplikasi Dompet Digital dalam Kehidupan Sehari-hari di Tangerang Selatan”, maka dapat disimpulkan beberapa hal sebagai berikut: Tingkat Pemahaman Masyarakat Masih Beragam Sebagian masyarakat sudah memahami bahwa penggunaan dompet digital memiliki potensi risiko seperti penipuan online, kebocoran data pribadi, dan kesalahan transaksi. Namun, masih ada sebagian pengguna yang belum memahami secara mendalam tentang fitur-fitur keamanan yang tersedia di aplikasi dompet digital. Risiko yang Sering Dihadapi Pengguna Risiko yang paling sering dialami adalah pesan phishing atau penipuan yang meminta kode OTP, kesalahan transfer saldo, dan kekhawatiran terhadap kebocoran data pribadi. Faktor utama penyebab risiko ini adalah kurangnya kewaspadaan pengguna dan rendahnya literasi digital. Strategi Mitigasi Sudah Mulai Diterapkan, Tapi Belum Optimal Sebagian besar pengguna telah melakukan langkah dasar seperti tidak membagikan OTP, menggunakan kata sandi kuat, dan memperbarui aplikasi secara berkala. Namun, penerapan verifikasi dua langkah (2FA) dan penggunaan fitur keamanan tambahan masih belum maksimal. Pentingnya Edukasi dan Literasi Keamanan Digital Peningkatan pengetahuan masyarakat tentang keamanan digital dapat membantu menurunkan risiko kejahatan siber. Edukasi dapat dilakukan melalui kampanye digital, sosialisasi oleh pihak penyedia layanan, maupun program literasi digital di masyarakat.

Referensi

- [1] Bank Indonesia, “Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia,” Jakarta, 2024.
- [2] Bank Indonesia, “Peraturan Anggota Dewan Gubernur Nomor 24 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia,” Jakarta, 2024.
- [3] D. F. Harseno and D. Achjari, “Analisis faktor-faktor yang memengaruhi penggunaan e-wallet di Indonesia,” *ABIS: Accounting and Business Information Systems Journal*, vol. 9, no. 4, 2021, doi: 10.22146/abis.v9i4.70384.
- [4] S. Suryati and I. Yoga, “The influence of perceived ease of use, trust and security on intention to use e-wallet,” *Journal of Management and Islamic Finance*, vol. 1, no. 2, pp. 294–308, 2021, doi: 10.22515/jmif.v1i2.4692.
- [5] D. Hidayat, C. H. Pangaribuan, O. P. B. Putra, and F. J. Taufiq, “Expanding the technology acceptance model with the inclusion of trust and mobility to assess e-wallet user behavior: Evidence from OVO consumers in Indonesia,” *IOP Conference Series: Earth and Environmental Science*, vol. 729, art. no. 012050, 2021, doi: 10.1088/1755-1315/729/1/012050.
- [6] A. Ciptarianto and Y. Anggoro, “E-wallet application penetration for financial inclusion in Indonesia,” *International Journal of Current Science Research and Review*, vol. 5, no. 2, pp. 319–332, 2022, doi: 10.47191/ijcsrr/V5-i2-03.
- [7] M. A. Hassan and Z. Shukur, “Device identity-based user authentication on electronic payment system for secure e-wallet apps,” *Electronics*, vol. 11, no. 1, art. no. 4, 2022, doi: 10.3390/electronics11010004.

- [8] M. U. Fadhilla and E. N. Purwanto, "The effect of digital literacy and perceptions of personal data security on the decision to use e-wallet as a payment system in MSMEs in the Jakarta area," *Journal of Management and Energy Business*, vol. 2, no. 2, 2023, doi: 10.54595/jmeh.v2i2.29.
- [9] Elvi, "Faktor yang memengaruhi penggunaan dompet digital di Indonesia," *Jurnal Manajemen Bisnis dan Kewirausahaan*, vol. 7, no. 1, 2023, doi: 10.24912/jmbk.v7i1.22476.
- [10] S. Houy, P. Schmid, and A. Bartel, "Security aspects of cryptocurrency wallets—A systematic literature review," *ACM Computing Surveys*, vol. 56, no. 1, art. no. 4, pp. 1–31, 2023, doi: 10.1145/3596906.
- [11] Y. E. Rachmad, A. A. Bakri, R. Nuraini, T. W. Nurdiani, and Kushariyadi, "Application of the Unified Theory of Acceptance and Use of Technology method to analyze factors influencing the use of digital wallets in Indonesia," *Jurnal Informasi dan Teknologi*, vol. 6, no. 1, 2024, doi: 10.60083/jidt.v6i1.504.
- [12] D. Dharmawan, H. Rusman, U. W. Nuryanto, P. A. Cakranegara, and M. Munizu, "Analysis of the influence of perceive of benefit, digital security, and perceived ease of use on intention to purchase using the digital wallet application," *Jurnal Informasi dan Teknologi*, vol. 6, no. 2, pp. 12–17, 2024, doi: 10.60083/jidt.v6i2.523.
- [13] F. R. Prawira, N. T. Prakoso, P. W. Handayani, and N. C. Harahap, "The influence of information security factors on the continuance use of electronic wallet," *Procedia Computer Science*, vol. 234, pp. 1467–1475, 2024, doi: 10.1016/j.procs.2024.03.147.
- [14] "Impact of security on wallet adoption: Multiple and serial mediating roles of trust and attitude and gender as a moderator," *International Journal of Bank Marketing*, vol. 42, no. 5, pp. 870–896, 2024, doi: 10.1108/IJBM-02-2023-0118.
- [15] F. S. Khalida, L. Budiarti, A. Arninda, and M. A. Madepo, "Impact of digital financial literacy, perceived ease of use, perceived usefulness, perceived security and social influence on intention to use e-wallet for students in Pontianak City," in *Proceedings of the 1st International Conference on Economics and Business*, 2024, doi: 10.4108/eai.2-8-2023.2341489.
- [16] N. A. B. Sinulingga, P. Ginting, B. K. F. Sembiring, and A. S. Silalahi, "A study intention, implementation and adoption of e-wallet in Indonesia," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 11, art. no. 8857, 2024, doi: 10.24294/jipd.v8i11.8857.
- [17] P. D. Persadha et al., "Exploring the factors influencing e-wallet adoption in Indonesia: An extended technology acceptance model approach," *Journal of Logistics, Informatics and Service Science*, vol. 11, no. 9, pp. 484–498, 2024, doi: 10.33168/JLISS.2024.0929.
- [18] F. Nursjanti, L. Amaliawati, and I. Nilasari, "Examining the determinants of Gen Z's continuance intention towards e-wallets," *International Journal of Management and Economics Invention*, vol. 10, no. 12, 2024, doi: 10.47191/ijmei/v10i12.12.
- [19] Bank Indonesia, *Statistik Sistem Pembayaran Indonesia 2023*, Jakarta: Bank Indonesia, 2023.
- [20] Otoritas Jasa Keuangan, *Laporan Fintech dan Inovasi Digital Keuangan di Indonesia*, Jakarta: OJK, 2023.
- [21] Kementerian Komunikasi dan Informatika RI, *Literasi Digital Nasional: Panduan Keamanan Transaksi Online*, Jakarta: Kominfo, 2024.
- [22] Sugiyono, *Metode Penelitian Kualitatif, Kuantitatif, dan R&D*, Bandung: Alfabeta, 2019.
- [23] D. Rahmawati, "Analisis penggunaan dompet digital dan tingkat keamanan pengguna di Indonesia," *Jurnal Teknologi dan Keuangan Digital*, vol. 4, no. 2, pp. 45–53, 2022.
- [24] A. Prasetyo and M. Lestari, *Perilaku Konsumen dalam Penggunaan E-Wallet di Era Digital*, Yogyakarta: Deepublish, 2021.
- [25] CNBC Indonesia, "Transaksi dompet digital naik 40%, tapi risiko keamanan masih tinggi," 12 Mar. 2024.
- [26] Katadata.co.id, "Riset penggunaan e-wallet oleh masyarakat Indonesia," 5 May 2024.