Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 201-212
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Strategi Manajemen Sekuriti Untuk Meningkatkan Kepercayaan Pengguna Terhadap Transaksi E-Wallet

Artha Bangkit Auliano [1,*], Filemon Leonardo Dongoran [1], Mohammad Diandra Ferdiansyah [1], Rasyid Darusman [1], Sandy Fitriansyah [1]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Perjuangan No. 81 Bekasi Utara, (021) 889558822; e-mail: 202310715068@mhs.ubharajaya.ac.id, 202310715327@mhs.ubharajaya.ac.id, 202210715118@mhs.ubharajaya.ac.id, 202210715145@mhs.ubharajaya.ac.id, 202310715099@mhs.ubharajaya.ac.id

Korespondensi: e-mail: 202310715068@mhs.ubharajaya.ac.id

Diterima: 2 Jan 25; Review: 4 Jan 25; Disetujui: 9 Jan 25; Diterbitkan: 9 Jan 25

Abstract

Abstract: Implementing a security management strategy is essential to ensure the security of electronic transactions, particularly in the use of digital wallets. E-wallets have become one of the most popular solutions for conducting online transactions, but they are often vulnerable to cyber-attacks and identity theft. This paper aims to examine security management strategies and practices that can be used to strengthen user protection in e-wallet transactions. The methods applied include literature review and data collection to identify security threats often faced by e-wallet users and mitigation measures that can be taken to reduce these risks. The strategies discussed include data encryption, double authentication, suspicious transaction monitoring, and user training on digital security practices. It is expected that the understanding and implementation of these security management practices will provide better protection for e-wallet users and increase their confidence in utilizing electronic transaction services.
***Keywords**: Security Management,E-Wallet Transactions,Digital Security,Electronic Payment Systems*

Abstrak

Abstrak: Pelaksanaan strategi manajemen keamanan sangat penting untuk memastikan keamanan transaksi elektronik, khususnya dalam penggunaan dompet digital. Dompet elektronik menjadi salah satu solusi yang populer untuk melakukan transaksi daring, tetapi sering kali rentan terhadap serangan siber dan pencurian identitas. Tulisan ini bertujuan untuk meneliti strategi dan praktik pengelolaan keamanan yang dapat digunakan untuk memperkuat perlindungan pengguna pada transaksi e-wallet. Metode yang diterapkan mencakup kajian literatur dan pengumpulan data guna mengidentifikasi ancaman keamanan yang sering dihadapi oleh pengguna e-wallet serta tindakan mitigasi yang bisa dilakukan untuk menekan risiko tersebut. Berbagai strategi yang dibahas mencakup enkripsi data, otentikasi ganda, pengawasan transaksi mencurigakan, serta pelatihan pengguna mengenai praktik keamanan digital. Diharapkan bahwa pemahaman dan implementasi praktik manajemen keamanan ini akan memberikan perlindungan yang lebih baik untuk pengguna e-wallet dan meningkatkan kepercayaan mereka dalam memanfaatkan layanan transaksi elektronik.
Kata kunci: Manajemen sekuriti,Keamanan Pengguna,Transaksi E-wallet,Sistem Pembayaran Digital

1. Pendahuluan

Di tengah pesatnya perkembangan teknologi informasi, sistem pembayaran digital telah mengalami transformasi besar, salah satunya melalui hadirnya e-wallet atau dompet digital. E-wallet memberikan kemudahan luar biasa bagi pengguna untuk melakukan berbagai transaksi keuangan, seperti pembayaran tagihan, pembelian barang dan jasa, hingga pengiriman uang. Kemajuan teknologi ini tidak hanya mendorong efisiensi dalam sistem pembayaran, tetapi juga mengubah kebiasaan masyarakat dalam bertransaksi secara signifikan.

Penelitian ini bertujuan untuk memberikan pemahaman tentang konteks penggunaan platform e-wallet di Indonesia, dengan fokus pada keamanan transaksi dan kepercayaan pengguna. Sebagai negara dengan populasi yang semakin mengadopsi teknologi finansial, Indonesia mengalami pertumbuhan pesat dalam penggunaan e-wallet. Fenomena ini tercermin dalam peningkatan jumlah pengguna dan transaksi melalui platform e-wallet tertentu mencakup seluruh wilayah Indonesia (Kusumawardhani & Purnaningrum, 2023).

Secara global, platfrom e-wallet telah menjadi pendorong utama perubahan dalam perilaku transaksi penjual (seller) dan pembeli (buyer), membawa kemudahan dalam melakukan transaksi tanpa menggunakan uang tunai dan meningkatkan aksesibilitas ke layanan keuangan (Sulthon & R, 2021) . Namun, di balik kemudahan tersebut, muncul berbagai tantangan yang berkaitan dengan aspek keamanan. Ancaman seperti pencurian data pribadi, peretasan akun, hingga serangan malware menjadi risiko serius yang dihadapi oleh pengguna e-wallet. Dengan semakin meningkatnya volume transaksi online, kepercayaan pengguna terhadap keamanan layanan ini menjadi faktor kunci yang memengaruhi adopsi teknologi e-wallet secara luas.

Pentingnya manajemen keamanan dalam transaksi e-wallet tidak dapat diabaikan. Upaya untuk melindungi data dan transaksi pengguna memerlukan pendekatan yang komprehensif, mulai dari penerapan teknologi keamanan seperti enkripsi dan autentikasi, hingga penyusunan kebijakan dan prosedur yang sesuai dengan standar industri. Dengan strategi yang tepat, layanan e-wallet tidak hanya mampu meningkatkan pengalaman pengguna tetapi juga membangun kepercayaan di era digital yang terus berkembang.

Pendahuluan ini bertujuan untuk mengeksplorasi peran penting manajemen keamanan dalam e-wallet, mengidentifikasi tantangan utama yang dihadapi, serta menyajikan strategi terbaik untuk memastikan perlindungan data dan transaksi pengguna. Dengan pemahaman yang lebih mendalam, diharapkan layanan e-wallet dapat menjadi platform yang lebih aman dan terpercaya dalam mendukung kebutuhan transaksi digital masyarakat.

2. Metode Penelitian

Penelitian ini melakukan tinjauan terhadap literatur yang relevan untuk memahami kerentanan keamanan pada transaksi e-wallet dan berbagai strategi manajemen sekuriti yang telah diusulkan atau diterapkan sebelumnya. Dengan cara mengumpulkan data koresponden dari pengguna transaksi e-wallet yang telah mengalami serangan atau penipuan sebelumnya untuk memahami modus operasi yang umum digunakan oleh penyerang untuk menganalisis kasus-kasus keamanan yang sukses dan tidak berhasil dalam implementasi manajemen sekuriti pada transaksi e-wallet. Menggunakan teknik analisis kualitatif untuk mendapatkan pemahaman yang komprehensif tentang isu-isu tersebut (Azhari et al., 2023).

3. Hasil dan Pembahasan

Pada bagian ini, hasil penelitian disajikan dalam bentuk gambar untuk memberikan gambaran yang lebih jelas dan terstruktur. Penyajian ini mencakup analisis kebutuhan hingga pengolahan data, disusun secara sistematis sesuai dengan tujuan penelitian.

3.1. Hasil Penelitian

Penelitian ini dilakukan untuk mengidentifikasi tingkat Kepercayaan Pengguna Terhadap Transaksi E-Wallet Berdasarkan survei yang telah dilakukan bersama dengan total 126 responden, berikut ini adalah beberapa hasil table pada setiap pertanyaan yang sudah di berikan :

3.1.1. Pengalaman Dalam Menggunakan E-Wallet

a. **Pertanyaan Nomor 1 : Berapa lama anda dalam menggunakan E-Wallet ?**

	Berapa Pengalaman Anda Dalam Menggunakan E-Wallet	Record Count
1.	1-3 tahun	57
2.	Lebih dari 3 tahun	47
3.	Kurang dari 1 tahun	22

Sumber : Hasil Penelitian (2024)

Gambar 1. Hasil Pertanyaan nomor 1

Pada gambar 1 menunjukan data survel yang telah di kumpulan rata-rata orang sudah memakai E-Wallet lebih dari 1 tahun sebanyak 82,5 % bahkan yang memakai E-Wallet lebih dari tiga tahun cukup banyak sebanyak 37,3 % dari jumlah data yang di kumpulkan.

3.1.2. Aplikasi E-Wallet Yang Digunakan

b. Pertanyaan nomor 2 : Aplikasi E-Wallet apa yang anda gunakan ?

	Aplikasi e-wallet apa yang anda gunakan?	Record Count
1.	Dana	40
2.	Gopay	37
3.	OVO	28
4.	Shopee Pay	17
5.	Pay Pal	1
6.	semua nya	1
7.	dw	1
8.	gopay dan dana	1

Sumber : Hasil Penelitian (2024)

Gambar 2. Hasil Pertanyaan nomor 2

Pada gambar 2 menunjukan data survei yang telah di kumpulan Aplikasi E-Wallet yang paling banyak di gunakan oleh orang-orang adalah Aplikasi Dana sebanyak 31,75 % dan yang paling sedikit adalah Pay Pal, dan yang memakai semua E-Wallet sebanyak 0,79 %.

3.1.3. Seberapa Sering Penggunaan E-Wallet

c. Pertanyaan nomor 3 : Seberapa sering anda menggunakan E-Wallet untuk transaksi?

	Seberapa sering Anda menggunakan E-Wallet untuk transaksi?	Record Count
1.	Beberapa kali seminggu	58
2.	Beberapa kali sebulan	27
3.	Jarang	21
4.	Setiap hari	20

Sumber : Hasil Penelitian (2024)

Gambar 3. Hasil Pertanyaan nomor 3

Pada gambar 3 menunjukan data survei telah di kumpulan E-Wallet paling banyak di gunakan dalam beberapa kali seminggu yaitu sebanyak 46,03 % dan paling jarang di gunakan yaitu setiap hari yaitu sebanyak 15,87 %.

3.1.4. Alasan Utama Penggunaan E-Wallet

d. Pertanyaan nomor 4 : Apa alasan utama anda menggunakan E-Wallet?

	Apa alasan utama Anda menggunakan e-wallet?	Record Count
1.	Kemudahan dalam transaksi	95
2.	Kecepatan dalam transaksi	20
3.	Keamanan dalam transaksi	10
4.	null	1

Sumber : Hasil Penelitian (2024)

Gambar 4. Hasil Pertanyaan nomor 4

Pada gambar 4 menunjukan data survei yang telah di kumpulan alasan utama pengguna menggunakan E-Wallet adalah untuk kemudahan dalam transaksi yaitu sebanyak 75,40 %.

3.1.5. Keamanan Penggunaan E-Wallet

e. Pertanyaan nomor 5 : Seberapa aman anda merasa menggunakan E-Wallet saat ini?

	Seberapa aman Anda merasa menggunakan e-wallet saat ini?	Record Count
1.	Sangat aman	66
2.	Aman	55
3.	Tidak aman	4
4.	Sangat tidak aman	1

Sumber : Hasil Penelitian (2024)

Gambar 5. Hasil Pertanyaan nomor 5

Pada gambar 5 menunjukan data survei yang telah di kumpulan seseorang merasa sangat aman untuk menggunakan E-Wallet saat ini sebanyak 52,38% dan hanya 0,8% seseorang merasa sangat tidak aman untuk menggunakan E-Wallet.

f. Pertanyaan nomor 6 : Apakah anda pernah mengalami masalah keamanan saat menggunakan E-Wallet ?

	Apakah Anda pernah mengalami masalah keamanan saat menggunakan e-wallet?	Record Count
1.	Tidak Pernah	71
2.	Pernah	55

Sumber : Hasil Penelitian (2024)

Gambar 6. Hasil Pertanyaan nomor 6

Pada gambar 6 menunjukan data survei yang telah di kumpulan rata-rata pengguna tidak memiliki masalah keamanan saat menggunakan E-Wallet yaitu sebanyak 56,35 % dan 43,7% rata-rata pengguna memiliki masalah keamanan saat menggunakan E-Wallet

g. Pertanyaan nomor 7 : Apakah anda mengetahui langkah-langkah keamanan yang disarankan untuk penggunaan E-Wallet?

	Apakah Anda mengetahui langkah-langkah keamanan yang disarankan untuk penggunaan e-wall...	Record Count
1.	Ya	112
2.	Tidak	14

Sumber : Hasil Penelitian (2024)

Gambar 7. Hasil Pertanyaan nomor 7

Pada gambar 7 menunjukan data survei yang telah di kumpukan sebanyak 88,9% pengguna sudah mengetahui tentang langkah-langkah keamanan dalam penggunaan E-Wallet dan 11,1% pengguna belum mengetahui tentang langkah-langkah keamanan dalam penggunaan E-Wallet.

h. Pertanyaan nomor 8 : Seberapa sering anda mengikuti berita atau informasi mengenai keamanan siber ?

	Seberapa sering Anda mengikuti berita atau informasi mengenai keamanan siber?	Record Count
1.	Sangat sering	49
2.	Sering	44
3.	Jarang	30
4.	Tidak pernah	3

Sumber : Hasil Penelitian (2024)

Gambar 8. Hasil Pertanyaan nomor 8

Pada gambar 8 menunjukan data survei yang telah dikumpukan yaitu sebanyak 38,9% pengguna sudah mengetahui informasi mengenai kemanan siber dan 2,4% pengguna tidak pernah mengetahui informasi mengenai kemanan siber.

i. Pertanyaan nomor 9 : Apa tindakan yang anda lakukan untuk menjaga akun E-Wallet anda ?

	Apa tindakan yang Anda lakukan untuk menjaga keamanan akun e-wallet Anda?	Record Count
1…	Mengaktifkan otentikasi dua faktor	63
2…	Memeriksa laporan transaksi secara rutin	32
3…	Mengganti password secara berkala	23
4…	Tidak menggunakan Wi-Fi publik	6
5…	null	2

Sumber : Hasil Penelitian (2024)

Gambar 9. Hasil Pertanyaan nomor 9

Pada gambar 9 menunjukan data survei yang telah di kumpulan tindakan yang paling banyak di ambil untuk menjaga keamanan akun E-Wallet adalah dengan mengaktifkan autentikasi dua faktor sebanyak 50 %.

3.2. Pembahasan

3.2.1. Manajemen Sekuriti

Keamanan merupakan upaya komprehensif untuk melindungi aset-aset penting suatu organisasi dari berbagai ancaman, kerentanan, dan risiko yang mungkin timbul. Aset ini mencakup informasi sensitif, infrastruktur TI, perangkat keras, perangkat lunak, jaringan, dan sumber daya lain yang penting bagi operasi organisasi. Proses manajemen keamanan dimulai dengan penilaian risiko, di mana organisasi mengidentifikasi potensi ancaman, kerentanan sistem, dan. potensi dampak dari peristiwa yang merugikan. Berdasarkan penilaian ini, organisasi merancang kebijakan, prosedur, dan praktik keamanan yang sesuai. Hal ini mencakup pengembangan aturan, pedoman, dan langkah-langkah untuk mengelola akses, melindungi data, dan merespons insiden keamanan (Azhari et al., 2023).

Pengendalian akses merupakan bagian penting dari manajemen sekuriti, yang memastikan bahwa hanya orang yang diotorisasi yang dapat mengakses aset yang sensitif. Ini melibatkan penggunaan otentikasi, otorisasi berbasis peran, dan monitoring aktivitas pengguna. Selain itu, organisasi juga menerapkan teknologi keamanan seperti firewall, antivirus, enkripsi, dan deteksi intrusi untuk mencegah serangan dan kebocoran data. Meningkatnya serangan siber dan pembobolan data dalam beberapa tahun terakhir telah meningkatkan kekhawatiran pengguna Internet. Oleh karena itu, pengelolaan data pengguna memerlukan kontrol keamanan yang lebih kuat dan canggih (Ningrum et al., 2023) . Pelatihan dan kesadaran merupakan elemen kunci dari manajemen keamanan, dimana organisasi mendidik karyawan mengenai praktik keamanan yang baik dan membuat mereka sadar akan ancaman keamanan yang ada. Manajemen insiden

juga merupakan aspek penting, membantu organisasi bersiap menangani insiden keamanan dengan cepat dan efektif (Azhari et al., 2023).

Manajemen keamanan adalah pendekatan komprehensif yang mencakup kombinasi strategi, kebijakan, prosedur, teknologi, pelatihan, dan pemantauan untuk melindungi aset penting organisasi. banyak ancaman dan risiko keamanan. Hal ini memungkinkan organisasi untuk menjaga kelangsungan operasional, menjaga reputasi, dan memenuhi kebutuhan pemangku kepentingan (Azhari et al., 2023).

3.2.2. Keamanan

Keamanan adalah suatu kondisi atau situasi di mana individu, organisasi, atau sistem dilindungi dari berbagai risiko, ancaman, atau bahaya yang mungkin timbul. Konsep ini mencakup upaya proaktif dan preventif untuk mengidentifikasi, mencegah, mengurangi, atau mengatasi potensi ancaman terhadap aset atau kepentingan yang bernilai. Risiko keamanan dalam penggunaan uang elektronik dapat terjadi dalam bentuk pencurian, penggandaan kartu asli, modifikasi data atau aplikasipada kartu asli, dan lain-lain (Sari et al., 2020).

Dalam konteks keamanan informasi dan teknologi, seperti e-wallet, keamanan melibatkan perlindungan terhadap integritas, kerahasiaan, dan ketersediaan data serta layanan yang dikomunikasikan, disimpan, atau diproses oleh sistem elektronik. Sistem pembayaran digital ini memberikan dampak yang signifikan terhadap keputusan pembelian, dan penggunaan media elektronik seperti smartphone telah meningkatkan minat dalam mengambil keputusan pembelian (Achmad Fauzi et al., 2022) . Keamanan e-wallet mengacu pada semua tindakan, prosedur, dan teknologi yang diterapkan untuk melindungi informasi keuangan dan identitas pengguna, serta memastikan keamanan transaksi keuangan yang dilakukan melalui platform dompet elektronik. Hal ini mencakup perlindungan terhadap akses tidak sah, penggunaan data tidak sah, manipulasi transaksi, dan ancaman keamanan lainnya yang dapat mengancam kelangsungan operasi dan kepercayaan pengguna terhadap platform (Azhari et al., 2024).

3.2.3. E-Wallet

Uang elektronik adalah suatu alat pembayaran elektronik yang diperoleh dengan terlebih dahulu menyetorkan sejumlah uang tertentu kepada penerbit, baik secara langsung maupun melalui lembaga penerbit, atau dengan mendebit rekening bank dan mencatat nilai uang yang ada di dalamnya. Pembawa uang elektronik. Dinyatakan dalam satuan Rupiah dan digunakan untuk melakukan transaksi pembayaran dengan memotong langsung nilai mata uang pembawa uang elektronik (Hendarsyah, 2016). Nilai uang tersebut disimpan secara elektronik pada

server media atau chip dan digunakan sebagai alat pembayaran oleh pedagang yang bukan penerbit uang elektronik tersebut. Dompet elektronik adalah jenis teknologi keuangan yang membuat pembayaran lebih nyaman bagi konsumen (Susanti & Dwiana Putra, 2023). E-wallet termasuk dalam kategori aset keuangan yang disimpan di server media. E-wallet dapat digunakan melalui aplikasi digital dan juga dapatmenyimpan dana untuk melakukan transaksi pembayaran (Dirnaeni et al., 2021).

3.2.4. Sistem Pembayaran Digital

Memahami pembayaran adalah proses pertukaran mata uang untuk barang, jasa atau informasi. Pengertian pembayaran digital adalah suatu alat yang menggunakan teknologi melalui telepon seluler untuk melakukan pembayaran, mentransfer uang atau melakukan transaksi lainnya. Kemajuan teknologi dalam sistem pembayaran saat ini telah mengubah peran uang tunai sebagai alat pembayaran menjadi bentuk pembayaran nontunai atau elektronik yang lebih efisien dan ekonomis (Azhari et al., 2023).

3.2.5. Bentuk penerapan strategi Manajemen Sekuriti untuk Meningkatkan Kepercayaan Pengguna Terhadap Transaksi E-Wallet

Tujuan keamanan data adalah untuk menjaga kelangsungan bisnis dan mengurangi hilangnya nilai bisnis dengan membatasi dampak insiden keamanan (Saputra et al., 2024). Penerapan strategi manajemen sekuriti untuk meningkatkan kepercayaan pengguna terhadap transaksi ini memastikan perlindungan yang optimal terhadap informasi dan dana pengguna/user. Berikut adalah beberapa bentuk penerapannya manajemen sekuriti yang dapat meningkatkan keamanan e-wallet antara lain:

1. Enkripsi Data: Mengenkripsi data sensitif seperti informasi kartu kredit, nomor rekening bank, dan kata sandi/pin pengguna saat disimpan dan dikirimkan melalui jaringan.
2. Otentikasi multi-faktor: Memastikan bahwa setiap transaksi atau akses ke akun e-wallet anda memerlukan beberapa metode otentikasi, seperti kata sandi/pin, kode verifikasi yang dikirimkan melalui SMS atau email, atau bahkan biometric seperti sidik jari atau pengenalan wajah.
3. Pemantauan Transaksi: Menerapkan sistem pemantauan transaksi yang canggih untuk mendeteksi aktivitas mencurigakan atau tidak biasa yang mungkin mengindikasikan akses illegal atau penipuan.
4. Pembaharuan keamanan rutin: Pastikan platform e-wallet terus diperbarui dengan patch keamanan terbaru untuk mengtasi kerentanan yang baru ditemukan.

5. Pertahanan terhadap serangan cyber: Melindungi sistem e-wallet dari berbagai jenis serangan cyber seperti serangan phishing, serangan malware, serangan DDoS (denial of service), dan lain lain dengan menggunakan teknologi keamanan yang tepat.

Dengan menerapkan langkah-langkah ini secara efektif, penyedia layanan dompet elektronik dapat memastikan bahwa informasi dan dana pengguna tetap aman dan terlindungi dari ancaman keamanan yang ada maupun yang baru. Hal ini membantu membangun kepercayaan pengguna dan menjaga reputasi platform e-wallet.

3.2.6. Peran Penting Strategi Manajemen Sekuriti Untuk Meningkatkan Kepercayaan Pengguna Terhadap Transaksi E-Wallet

Manajemen sekuriti memiliki tanggung jawab utama dalam menjaga keamanan informasi sensitif pengguna, seperti nomor kartu kredit dan data pribadi lainnya. Preferensi menjadi hal penting dilakukan perusahaan-perusahaan e-wallet untuk mengetahui bagaimana atribut-atribut yang sesuai dengan kriteria atau pilihan yang paling diminati oleh para pengguna e-wallet (Perkasa, 2020).

4. Kesimpulan

Keamanan menjadi aspek yang sangat penting dalam penggunaan E-Wallet. Meskipun sebagian besar responden merasa aman atau sangat aman menggunakan platform ini, sebanyak 56,35% di antaranya pernah menghadapi masalah keamanan. Hal ini menunjukkan bahwa meskipun ada kepercayaan terhadap platform, ancaman keamanan tetap menjadi perhatian utama.

Kesadaran pengguna terhadap langkah-langkah keamanan juga tergolong tinggi, dengan 81,75% responden mengetahui cara melindungi akun mereka, seperti menggunakan autentikasi dua faktor (50%) dan rutin memeriksa laporan transaksi (25,39%). Hal ini mencerminkan dampak positif dari edukasi terkait keamanan digital yang semakin luas.

Selain itu, kepercayaan pengguna terhadap E-Wallet didorong oleh kombinasi kenyamanan dan keamanan. Sebanyak 75,40% responden menyebut kemudahan transaksi sebagai faktor utama, namun strategi keamanan seperti perlindungan data dan fitur keamanan tambahan juga memainkan peran penting dalam membangun kepercayaan.

Untuk memperkuat kepercayaan pengguna, platform E-Wallet perlu mengadopsi strategi keamanan yang lebih komprehensif. Beberapa langkah yang disarankan meliputi penerapan teknologi autentikasi canggih seperti biometrik, penguatan enkripsi data untuk melindungi informasi sensitif, edukasi berkelanjutan mengenai keamanan, pemberian notifikasi keamanan, serta layanan pelanggan yang responsif dalam menangani insiden keamanan.

Transparasi juga menjadi elemen penting dalam meningkatkan kepercayaan. Pengguna yang rutin mendapatkan informasi terkait keamanan siber cenderung lebih sadar akan risiko dan solusi yang tersedia.

Secara keseluruhan, kepercayaan pengguna terhadap E-Wallet sangat dipengaruhi oleh strategi keamanan yang diterapkan. Oleh karena itu, platform perlu proaktif dalam meningkatkan langkah-langkah keamanan, memberikan edukasi terkait risiko digital, serta menjamin kenyamanan layanan. Langkah-langkah ini diharapkan mampu memperkuat loyalitas dan kepercayaan pengguna terhadap platform E-Wallet.

Daftar Pustaka

Achmad Fauzi, Shifa Ashila Salwa, Aniar Safitri, Eka Amelia Chiesa Julianti, & Sindy Nur Fazriyah. (2022). ANALISIS PENGARUH PENGGUNAAN SISTEM PEMBAYARAN DIGITAL DAN DIGITAL MARKETING TERHADAP KEPUTUSAN PEMBELIAN. *Jurnal Ekonomi Dan Manajemen*, *2*(1), 11–17. https://doi.org/10.56127/jekma.v2i1.409

Azhari, F., Sumarno, S., Fauzi, A., Pratama, D. R., Musyafa, M. A., Nawawi, M. R., Shafly, N., & Ghaffar, A. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet. *Jurnal Kewirausahan Dan Multi Talenta*, *2*. https://doi.org/10.38035/jkmt.v2i2

Dirnaeni, D., Handrijaningsih, L., Mariani T.R, S., & Anisah, A. (2021). PERSEPSI KEMUDAHAN, CUSTOMER RELATIONSHIP MANAGEMENT DAN KUALITAS LAYANAN TERHADAP LOYALITAS PELANGGAN E-WALLET MELALUI. *Ultima Management : Jurnal Ilmu Manajemen*, 287–303. https://doi.org/10.31937/manajemen.v13i2.2203

Hendarsyah, D. (2016). Penggunaan Uang Elektronik Dan Uang Virtual Sebagai Pengganti Uang Tunai Di Indonesia. *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, *5*(1), 1–15. https://doi.org/10.46367/iqtishaduna.v5i1.74

Kusumawardhani, D. A., & Purnaningrum, E. (2023). Kusumawardhani and E. Purnaningrum, “Penyebaran Pengguna Digital Wallet Di Indonesia Berdasarkan Google Trends Analytics. *Semantic Scholar*.

Ningrum, D. A., Fauzi, A., Syaridwan, A., Putri, I. A., Putri, N. M., & Putri, S. A. (2023). Peran Manajemen Sekuriti Terhadap Keputusan Pembelian pada Pengguna Aplikasi Shopee (Studi Pustaka Manajemen Sekuriti). *Jurnal Ilmu Manajemen Terapan*, *4*. https://doi.org/10.31933/jimt.v4i5

Perkasa, H. R. (2020). ANALISIS PREFERENSI KONSUMEN DALAM MEMILIH ELECTRONIC WALLET (E-WALLET) DI KOTA BANDUNG ANALYSIS OF CONSUMER PREFERENCES IN CHOOSING ELECTRONIC WALLET (E-WALLET) IN BANDUNG CITY. *Skripsi*, *7*(2), 3536.

Saputra, F., Soesanto, E., Indah Cahyaningtyas, K., & Lukmanul Hakim, Z. (2024). Manajemen Security Terhadap Cyber Crime di Kominfo. *Indonesian Journal of Multidisciplinary*, *2*. https://journal.csspublishing/index.php/ijm

Sari, M. A., Listiawati, R., Novitasari, N., & Vidyasari, R. (2020). ANALISA PENGARUH DAYA TARIK PROMOSI, PERSEPSI KEMUDAHAN, PERSEPSI MANFAAT, PERSEPSI KEAMANAN TERHADAP MINAT PENGGUNAAN E-WALLET. *Ekonomi & Bisnis*, *18*(2), 126–134. https://doi.org/10.32722/eb.v18i2.2493

Sulthon, M. A., & R, A. P. (2021). Analisis KesadaranKeamanan di KalanganPengguna E-Wallet di Indonesia. *Universitas Islam Indonesia*, *2*.

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*, 407. https://doi.org/10.24843/EEB.2023.v12.i03.p05