KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research
Vol.2, No.4 Agustus 2024
e-ISSN: 3025-9851; p-ISSN: 3025-986X, Hal 108-116
DOI: https://doi.org/10.61722/jssr.v2i4.1955.

ANALISIS KEAMANAN DATA TERHADAP PENGGUNAAN E-WALLET SEBAGAI ALAT TRANSAKSI DIGITAL UNTUK MENCEGAH PENIPUAN ONLINE

Laksamana Khaidir K.N
laksakhaidir@gmail.com
Universitas Islam Negeri Sumatera Utara
Muhammad Irwan Padli Nasution
Irwannst@uinsu.ac.id.
Universitas Islam Negeri Sumatera Utara
Fakultas Ekonomi dan Bisnis Islam UINSU Medan
Korespondensi penulis : laksakhaidir@gmail.com.

ABSTRACT *Technological developments have changed the way people shop in general, from previously retail shopping to online shopping, which is more efficient and practical. Data security in online shopping transactions is a crucial issue in the digital era which continues to develop rapidly. As consumer interest in shopping online increases, the popularity of e-wallets is also increasing among the public. However, the higher the public's interest in shopping online, the higher the risk of online fraud, especially in digital transactions. This research aims to analyze data security in online shopping transactions using e-wallets and develop strategies or ways to prevent online fraud.This research aims to analyze various aspects of data security in online shopping transactions and find out how this can prevent online fraud. The main objectives of this research are to identify common security threats, effective data protection techniques and methods, and implement security policies that increase consumer confidence in online transactions.The research method used is a literature review and secondary data analysis. The research results show that the e-wallet system is equipped with strong security mechanisms such as data encryption, user authentication, and transaction validation. However, risks remain if users do not follow good security practices, such as: For example, using secure devices, updating software, and watching out for phishing scams. Therefore, preventing online fraud in purchase transactions via e-wallets requires increased user awareness, strict security policies, and cooperation with governments, service providers, and the public.*
Keywords: *Data security, Online Fraud, E-Wallet*

ABSTRAK Perkembangan teknologi telah mengubah cara berbelanja masyarakat pada umumnya yang sebelumnya masih berbelanja ritel menjadi belanja online yang dimana lebih efisien dan praktis. Keamanan data dalam transaksi belanja online merupakan isu krusial di era digital yang terus berkembang pesat. Seiring meningkatnya minat konsumen untuk berbelanja online popularitas e-wallet juga meningkat di kalangan para masyarakat. Namun semakin tingginya minat masyarakat untuk berbelanja online semakin tinggi juga risiko terjadinya penipuan online khususnya pada transaksi digital. Penelitian ini bertujuan untuk menganalisis keamanan data dalam transaksi belanja online menggunakan e-wallet dan mengembangkan strategi atau cara untuk mencegah penipuan online.Tujuan dari penelitian ini adalah untuk menganalisis berbagai aspek dari keamanan data dalam transaksi belanja online dan mengetahui bagaimana hal tersebut dapat mencegah penipuan online. Tujuan utama dari penelitian ini adalah untuk mengidentifikasi ancaman keamanan umum, teknik dan metode perlindungan data yang efektif, dan menerapkan kebijakan keamanan yang meningkatkan kepercayaan konsumen dalam transaksi online.Metode penelitian yang digunakan adalah tinjauan pustaka dan analisis data sekunder. Hasil penelitian menunjukkan bahwa sistem e-wallet dilengkapi dengan mekanisme keamanan yang kuat seperti enkripsi data, otentikasi pengguna, dan validasi transaksi. Namun, risiko tetap ada jika pengguna tidak mengikuti praktik keamanan yang baik, seperti: Misalnya, menggunakan perangkat yang aman, memperbarui perangkat lunak, dan hati-hati terhadap penipuan phishing. Oleh karena itu, mencegah

Received Juni 30, 2024; Revised Juli 02, 2024; Agustus 04, 2024
* Laksamana Khaidir K.N, *laksakhaidir@gmail.com*

penipuan online dalam transaksi pembelian melalui e-wallet memerlukan peningkatan kesadaran pengguna, kebijakan keamanan yang ketat, dan kerja sama dengan pemerintah, penyedia layanan, dan masyarakat.
Kata Kunci: Keamanan data, Penipuan Online, E-Wallet

PENDAHULUAN

Perkembangan teknologi informasi pada era sekarang terus mengalami kemajuan yang signifikan. Pesatnya kemajuan teknologi informasi telah membawa perubahan signifikan di berbagai sektor seperti perekonomian, pendidikan, kemasyarakatan, dan aspek sosial. Hal ini disebabkan oleh kemudahan penggunaan teknologi informasi dari berbagai sumber di seluruh negara. Teknologi dan informasi ini dapat diakses oleh siapa saja dan dimana saja melalui internet. Internet adalah jaringan elektronik global yang menggunakan teknologi satelit untuk menghubungkan komputer-komputer terorganisir di seluruh dunia. Pada saat ini, Internet telah menjadi alat penting bagi masyarakat umum di banyak negara, termasuk Indonesia. Hampir seluruh lapisan masyarakat optimis terhadap pertumbuhan Internet di Indonesia.

Selain itu kemajuan teknologi juga bisa di ibaratkan seperti pisau bermata dua yang dimana tidak hanya mempermudah segala aspek kehidupan penggunanya, namun bisa juga dipakai untuk tujuan-tujuan yang negatif yang pada akhirnya dapat merugikan orang banyak, seperti penipuan online. Terkait bisnis digital (e-commerce), e-commerce kini telah menjadi tren sosial, dan seiring dengan perkembangan teknologi, akan terjadi pergeseran besar-besaran dari perdagangan tradisional ke e-commerce.

Proses transisi ke digital system sudah mengubah persepsi masyarakat, termasuk sistem pembayaran. Sistem Pembayaran merupakan salah satu aspek terpenting di negara mana pun karena merupakan aspek fundamental yang mempengaruhi pertumbuhan dan pertumbuhan perekonomian nasional. Efektivitas sistem pembayaran dapat ditunjukkan oleh kemampuan negara dalam menghasilkan tarif minimum untuk menutupi biaya dan kerugian yang terkait dengan kegiatan bisnis yang menggunakan sistem pembayaran rahasia sebagai alat tukar dalam transaksi ekonomi. Uang merupakan alat transaksi utama yang digunakan oleh masyarakat di seluruh dunia. Pada saat ini mayoritas masyarakat menggunakan mata uang elektronik atau "e-money". Meningkatnya penggunaan mata uang elektronik di Indonesia merupakan hasil dari program GNNT (Gerakan Nasional Non Tunai) yang berupaya untuk meningkatkan pemahaman dan memberi edukasi kepada masyarakat akan risiko yang terkait dengan melakukan pembayaran keuangan melalui media non tunai.

Dikarenakan semakin seringnya masyarakat menggunakan internet untuk berbelanja online maka terbitlah layanan dompet digital yang saat ini menjadi sebuah kebiasaan masyarakat untuk bertransaksi ketika berbelanja online. Penggunaaan dompet digital ini juga sangat memudahkan transaksi jual beli. Dengan menggunakan e-wallet masyarakat dapat melakukan pembayaran dengan metode code QR (Quick Response) tanpa memerlukan melalui pembayaran tunai lagi. Pembayaran menggunakan metode e-wallet ini sangat trending saat ini karena sangat praktis dan memudahkan transaksi jual beli barang atau jasa.

Tujuan pengembangan metode pembayaran melalui e-wallet adalah untuk berkolaborasi dengan penyedia layanan pembayaran yang menawarkan kode QR berbeda dari penyedia layanan pembayaran yang berbeda ketika pelanggan melakukan transaksi nontunai. Dari situlah muncul sebuah terobosan inovasi yang mendorong efisiensi transaksi jual beli suatu layanan barang atau jasa.

Tujuan pengembangan metode pembayaran melalui e-wallet adalah untuk berkolaborasi dengan penyedia layanan pembayaran yang menawarkan kode QR berbeda dari penyedia layanan pembayaran yang berbeda ketika pelanggan melakukan transaksi nontunai. Dari situlah muncul sebuah terobosan inovasi yang mendorong efisiensi transaksi jual beli suatu layanan barang atau jasa. Melihat situasi saat ini, dimana semakin banyak masyarakat yang ingin menggunakan sistem pembayaran digital melalui e-wallet dan ikut serta untuk berpartisipasi dalam inisiatif negara demi menerapkan transaksi cash-less, maka dapat disimpulkan jika orang-orang telah sadar akan manfaat, kemudahan dan kepraktisan aplikasi transaksi e-wallet. Keuntungan dari metode pembayaran yang disebutkan di atas.

Namun dibalik kemudahan dan keuntungan tersebut terdapat resiko pada keamanan data kita yang perlu dipertimbangkan ketika kita melakukan transaksi online menggunakan e-wallet yaitu seperti penipuan atau scam. Kejahatan online yang berjalan pada transaksi digital ialah contoh wujud utama pelanggaran hukum di dunia digital dan tentunya akan sulit untuk mengidentifikasi dan menangkap pelakunya. Pada awalnya, tantangan di ranah dunia digital terutama terbatas pada ruang fisik sebab, digital world merupakan dunia tanpa batasan (borderless world) yang memudahkan pelaku dalam memalsukan identitasnya.

Oleh karena itu keamanan data merupakan aspek yang paling penting dalam penggunaan e-wallet mengingat transaksi yang dilakukan menggunakan informasi dan data pribadi user. Resiko kebocoran data pribadi, pencurian identitas seperti SIM, Nomor Rekening, Kode Verifikasi, KTP dan informasi rahasia yang lainnya. Hal ini merupakan ancaman yang nyata terhadap penggunaan e-wallet. Mengingat para pelaku penipuan online dapat mengakses informasi sensitif pengguna, seperti nomor kartu kredit atau informasi rekening bank, untuk melakukan transaksi ilegal. Hal ini dapat mengakibatkan kerugian finansial yang signifikan bagi pengguna. Oleh sebab itu, penting untuk menganalisis prosedur-prosedur security yang telah di implementasikan oleh para penyedia aplikasi dompet elektronik untuk melindungi data pengguna dan mencegah terjadinya penipuan online.

METODE PENELITIAN

Metodologi yang dipakai dalam membuat artikel ilmiah ini adalah Tinjauan literatur atau (literature review). Tinjauan literatur adalah proses meninjau, menganalisis dan meninjau ulang bermacam sumber karya tulis yang sudah pernah diterbitkan oleh akademisi atau peneliti lain terkait pembahasan yang akan diteliti. Metode ini penting dalam proses penelitian karena dapat memberikan ide dan informasi yang relate mengenai pembahasan yang akan diteliti. Metode literatur review adalah pendekatan yang bermanfaat dalam membangun pemikiran yang lebih intens mengenai pembahasan penelitian yang akan dibahas dan mendeteksi peluang untuk penelitian baru yang bisa mengisi gap atau ruang kosong yang teridentifikasi.

HASIL DAN PEMBAHASAN

Keamanan data

Keamanan data adalah serangkaian ujicoba atau kebijakan dalam teknologi yang digunakan untuk menjaga data dari akses yang tidak sah, kerusakan, pengubahan, atau pencurian. Ini melibatkan berbagai metode dan alat untuk memastikan integritas, kerahasiaan, dan ketersediaan data, baik saat data disimpan, diproses, atau ditransmisikan. Terlebih lagi keamanan data dapat mencegah akses yang memiliki virus atau akses yang tidak di inginkan oleh komputer yang mencoba untuk mengambil informasi dari data pribadi Pencurian data merupakan salah satu tindak kriminal yang memakan banyak korban.

Dalam praktiknya terdapat berbagai jenis keamanan data yang bisa kita gunakan seperti autentikasi, Enkripsi, Kontrol akses data, Confidentiality dll.

Auntentikasi

Auntentikasi adalah prosedur untuk memastikan identifikasi atau otentikasi. Pada dasarnya, metode otentikasi ini merupakan tindakan pengamanan yang biasanya dapat mendeteksi pengguna secara tepat dan presisi sebelum memberikan izin untuk mereka dapat menjelajahi informasi yang relevan.

Enkripsi

Enkripsi adalah proses mengubah informasi atau data menjadi gambaran yang tidak bisa dibaca, dipahami, atau dikerjakan tanpa menggunakan keyboard atau metode decoding tertentu. Tujuan utama pengkodean adalah untuk melindungi integritas dan kerahasiaan data, sehingga hanya organisasi dengan akses dan pengetahuan yang sesuai yang dapat mengakses dan memahami informasi yang relevan.

Data access control

Data access control merupakan jenis aktivitas penjagaan yang menghambat seluruh celah ke dalam jaringan digital lainnya. Aspek ini terkait dengan kewenangan terhadap control data. Oleh sebab itu, sering kali hal ini berkaitan dengan masalah pribadi dan kerahasiaan. Dengan demikian, kontrol atas proses dilakukan melalui penggunaan ID pengguna dan kata sandi ID, atau metode alternatif.

Confidentiality

Confidentiality adalah metode untuk melindungi informasi rahasia milik seseorang yang tidak mempunyai hak akses. Informasi tersebut biasanya hanya dapat diakses oleh kelompok yang berwenang atau kelompok yang memiliki otorisasi. Kerahasiaan ini berkaitan dengan informasi yang diberikan kepada organisasi lain. Prinsip tersebut bertujuan untuk mengamankan data dari peretas yang tidak sah dan untuk menjaga kerahasiaannya.

Faktor penyebab terjadinya penipuan dalam transaksi online

Kasus kejahatan online pada transaksi digital sudah kerap kali kita temui. Para pelaku cyber crime biasanya akan mengaku dari pihak suatu e-commerce resmi, dan akan berpura-pura mengatur hadiah fiktif dengan iming-imingan khusus dengan meminta data rahasia para korban, bahkan bisa ke uang korban. Kejahatan dunia maya biasanya mempunyai jurus-jurus tertentu untuk menipu para korbannya.Akan tetapi, apasih faktor penyebab penipuan dalam transaksi online? Berikut inilah faktor-faktor yang menyebabkan terjadinya penipuan dalam transaksi digital berdasarkan tinjauan literatur:

1. Kebocoran data user

Ini biasanya akibat dari kesalahan kita sebagai pengguna. Penting untuk kita ingat bahwa informasi pribadi tidak boleh dibagikan, termasuk SIM, Nomor Rekening, Kode Verifikasi, KTP, dan informasi rahasia lainnya. Setelah data rahasia tersebar, mereka yang tidak bertanggung jawab bisa memakainya untuk upaya-upaya yang berbau kejahatan cyber. Disamping itu, kerusakan data juga bisa di akibatkan oleh peretas dan kebocoran data. Kelompok yang mampu menjalankan aspek ini umumnya adalah mereka yang memahami teknologi namun tidak menggunakannya dengan baik dan benar. Peretas juga dapat

memanfaatkan data kita dengan menggunakan tautan atau situs web. Oleh karena itu, jika kita menerima link atau email yang tidak jelas, jangan mengkliknya karena mungkin merupakan jebakan yang dibuat oleh peretas untuk melakukan tindakan penipuan online.

2. Faktor pengetahuan pengguna yang minim

Pada umumnya masyarakat membutuhkan edukasi untuk memahami risiko yang terkait dengan cybercrime melalui transaksi online. Mengingat di era digital sekarang ini mengharuskan semua orang menggunakan teknologi. Akan tetapi orang yang berusia lanjut belum tentu mahir menggunakan perangkat digital. Oleh sebab itu harus diterapkannya sosialisasi dan edukasi kepada seluruh warga negara untuk memahami gangguan kejahatan dalam digital transaksi. Melalui sosialisasi Kelompok ini, masyarakat perlahan akan mulai memahami pola motif penipuan dalam online transaction.

3. System keamanan dan kebijakan pemerintah relatif lemah

Seperti contoh kasus pada kebocoran data aplikasi e-commerce Tokopedia. Hal tersebut mengungkap tidak dapat diandalkannya sistem keamanan di Indonesia. Lemahnya posisi pemerintah dalam membuat kebijakan membuat para penjahat dunia maya mendapatkan keuntungan dalam hal ini. Namun di Indonesia sendiri, telah terdapat beberapa peraturan dan kebijakan keamanan informasi yang melindungi integritas online transaction. Akan tetapi, eksperimen khusus ini belum terbukti berhasil; hal ini dapat dijelaskan dengan tingginya tingkat cybercrime dalam transaksi online. Sebagai masyarakat umum, jika kita menerima kasus seperti itu, kita mempunyai kewajiban untuk melaporkannya kepada pihak yang berwenang guna mengurangi jumlah cybercrime dalam transaksi digital.

4. Tingginya tingkat kemiskinan dan pengangguran

Ketika orang-orang mengalami kesulitan ekonomi akibat pengangguran atau kemiskinan, mereka mungkin akan melakukan segala cara untuk mendapatkan uang. Aspek inilah yang menjadikan cikal bakal mereka terlibat dalam aktivitas cybercrime sebagai upaya untuk memperoleh uang melalui langkah yang praktis dan mudah. Ini dapat mendorong mereka untuk melakukan tindakan ilegal seperti penipuan, pencurian identitas, atau peretasan. Hanya dengan bermodal janji palsu, penipu transaksi online bisa melancarkan aksinya. Dalam hal ini tindakan penipuan dalam transaksi online ini harus diwaspadai oleh pemerintah. Dengan meningkatkan kesempatan kerja dan pengurangan kemiskinan sejalan dengan penurunan tindakan penipuan dalam online transaction.

Upaya Menjaga Keamanan Data Pelanggan

Tujuan keamanan data adalah untuk menjaga kelangsungan bisnis dan mengurangi hilangnya nilai bisnis dengan membatasi dampak insiden keamanan (L. A. Saputra et al., 2023. Upaya untuk menjaga keamanan data pelanggan merupakan kegiatan yang sangat penting untuk memastikan efektivitas data pengguna dan perlindungan informasi. Berikut adalah beberapa upaya untuk menjaga keamanan data pelanggan.

1. Otentikasi multi-faktor: Memastikan setiap transaksi atau akses ke akun e-wallet memerlukan setidaknya satu metode autentikasi, seperti kata sandi, kode terverifikasi email atau SMS, atau bahkan metode biometrik seperti sidik jari atau metode pengenalan wajah.

2. Pemantauan transaksi: Menginstall sistem pemantauan transaksi yang canggih untuk mendeteksi aktivitas tidak biasa yang dapat mengindikasikan adanya akses ilegal atau penipuan.
3. Enkripsi data: Penerapan enkripsi data yang benar sangat penting untuk melindungi privasi dan keamanan informasi dalam era digital saat ini. Hal ini membantu mencegah ancaman seperti pencurian data, pembobolan, dan penggunaan data secara tidak sah.
4. Perlindungan terhadap serangan cyber: Dengan menggunakan teknologi keamanan yang tepat, sistem dompet elektronik terlindungi dari beberapa jenis serangan siber, termasuk malware, phishing, dan serangan DDoS (Denial of Service).
5. Memastikan pembaruan sistem: Memastikan platform e-wallet terus diperbarui dengan sistem keamanan baru untuk mencegah dan mengatasi kerentanan sistem yang ditemukan oleh para tindak cybercrime.

Melalui penerapan prosedur ini secara efektif, penyedia dompet elektronik dapat menjamin bahwa data dan dana pengguna tetap aman dari risiko keamanan yang ada dan yang baru. Hal ini membantu pengguna mengembangkan kepercayaan pada platform dan mempertahankan reputasinya sebagai dompet elektronik.

Penegakan Hukum Terhadap Tindak Pidana Kejahatan Cyber

Penegakan hukum terhadap kejahatan cyber merupakan proses yang kompleks dan memiliki banyak aspek, mengingat kekhasan kejahatan semacam ini terkadang melibatkan penggunaan teknologi yang canggih yang bisa membobol sistem keamanan yang rapuh dalam pertahanan negara. Dalam hal ini negara kita telah membuat beberapa kebijakan hukum terkait kejahatan cyber yaitu sebagai berikut:

Undang-Undang Nomor 11 Tahun 2008

Pada pasal ini membahas mengenai Informasi dan Transaksi Elektronik (ITE) yang melarang cyber crime sehubungan dengan hukum privat. Saat ini, dalam Perjanjian ITE terdapat ketentuan terkait masalah kriminalisasi. Menurut Pasal 28 dan 29, siapa pun yang dengan sengaja dan melawan hukum menyebarkan informasi dan komunikasi palsu termasuk ancaman kekerasan terhadap individu akan dikenakan konsekuensi hukum. Selanjutnya berdasarkan 3 pasal tersebut menindaklanjuti pasal 45, diatur bahwa pelaku diancam dengan ancaman pidana paling lama enam tahun atau denda satu miliar rupiah. Pengetahuan Pidana tentang kejahatan yang memakai transaksi online ada dalam pasal XI tentang gejolak pidana yang terbentang dari pasal 45 hingga pasal 52.

UU No. 8 Tahun 1999

Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen di Indonesia merupakan regulasi yang dirancang untuk melindungi hak-hak konsumen dan menjamin keamanan serta kenyamanan mereka dalam bertransaksi. Pada Pasal 45-48 Mengatur tentang mekanisme penyelesaian perselisihan antara konsumen dan pemilik usaha, baik melalui pengadilan ataupun di luar pengadilan dan pada pasal Pasal 60-63 Menetapkan sanksi bagi para pelaku yang melanggar ketentuan dalam UU ini, yang bisa berupa sanksi administratif, pidana, atau perdata.

Undang-Undang Nomor 19 Tahun 2016

Tentang Perubahan Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008. Penggunaan teknologi informasi dan transaksi elektronik diatur dalam peraturan ini. Transaksi online termasuk di dalamnya. Undang-undang ini juga mengatur pelanggaran yang melibatkan penyalahgunaan teknologi informasi, termasuk pencurian identitas, penipuan online, dan pencurian data elektronik.

UU ITE

Sebagaimana yang telah tercantum di pasal 4 dijelaskan bahwa konsumen memiliki hak untuk memperoleh informasi yang akurat, jujur dan jelas. Apabila informasi tersebut belum cocok dengan haknya, konsumen memiliki hak untuk menuntut dan menempuh jalur hukum. Disamping itu, Kementerian Komunikasi dan Informatika (Kominfo) mempunyai kewenangan mengelola kasus seperti yang disebutkan di atas. Kominfo mempunyai tanggung jawab untuk melindungi kebocoran data publik yang mungkin dieksploitasi oleh kelompok yang tidak bertanggung jawab.

KESIMPULAN

Perkembangan teknologi telah mengubah cara berbelanja masyarakat dari sebelumnya belanja ritel menjadi belanja online yang lebih efisien dan praktis. Namun, kemudahan ini juga dapat digunakan oleh para peretas untuk melakukan penipuan online. Oleh sebab itu keamanan data dalam transaksi belanja online menggunakan e-wallet merupakan isu krusial di era digital yang terus berkembang pesat. Hasil penelitian menunjukkan bahwasannya e-wallet sendiri telah dilengkapi dengan mekanisme keamanan seperti enkripsi data, otentikasi pengguna, dan validasi transaksi. Namun, tetap ada risiko jika pengguna tidak menerapkan praktik keamanan yang baik, seperti menggunakan perangkat yang aman, memperbarui perangkat lunak, dan berhati-hati terhadap penipuan phishing. Langkah pencegahan penipuan online melalui e-wallet antara lain meningkatkan kesadaran pengguna, menerapkan kebijakan keamanan yang ketat, dan berkolaborasi dengan pemerintah, penyedia layanan, dan para masyarakat. Dengan demikian, dapat disimpulkan mengenai pentingnya keamanan data dalam transaksi online menggunakan e-wallet dan menekankan perlunya tindakan preventif untuk mencegah penipuan online.

DAFTAR PUSTAKA

Silalahi, P. R., Daulay, A. S., Siregar, T. S., & Ridwan, A. (2022). Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. *Profit: Jurnal Manajemen, Bisnis dan Akuntansi*, *1*(4), 224-235.

Soesanto, E., Utami, A. S., Chantica, J. A., Nabila, R. A., & Ricki, T. S. (2023). Keamanan Data Pribadi Dalam Sistem Pembayaran Via OVO Terhadap Ancaman dan Pengelabuan (Cybercrime). *IJM: Indonesian Journal of Multidisciplinary*, *1*(2).

Abdulloh, M. KEAMANAN DATA PRIBADI DALAM SISTEM PEMBAYARAN E-WALLET

Bodhi, S., & Tan, D. (2022). Keamanan Data Pribadi dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan dan Pengelabuan (Cybercrime). *UNES Law Review*, *4*(3), 297-308

Tara, I. K. K. B., & Sudiro, A. (2023). Perlindungan Hukum Konsumen Terhadap Pengguna Qris dan Penanganan Penipuan dalam Bertransaksi. *UNES Law Review*, *6*(2), 4581-4588.

Rustam, M. H., Hamler, H., Marlina, T., Handoko, D., & Alamsyah, R. (2023). Peran dan Tanggung Jawab Konsumen untuk Mencegah Praktik Penipuan dalam Transaksi Online dari Perspektif Hukum Perlindungan Konsumen. *Riau Law Journal*, *7*(1), 1-24.

Pardede, A., Setyabudi, C. M., & Nita, S. (2024). Penegakan Hukum terhadap Kasus Siber di Ditreskrimsus (Studi Kasus pada Polda Metro Jaya Tahun 2022). *Al Qalam: Jurnal Ilmiah Keagamaan dan Kemasyarakatan*, *18*(2), 1056-1069.

Rahmanto, T. Y., Kav, J. H. R. S., & Kuningan, J. S. (2019). Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum De Jure*, *19*(1), 31.

Birwin, A., Faridi, A., Furqan, M., Maryusman, T., & Seytawan, A. (2023). Descriptive Epidemiological Study of TB Occurrence in Matraman District Health Center Post Covid-19 Pandemic. *Jurnal Aisyah: Jurnal Ilmu Kesehatan*, *8*(2).

Azhari, F., Sumarno, S., Fauzi, A., Pratama, D. R., Musyafa, M. A., Nawawi, M. R., & Ghaffar, N. S. A. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet. *Jurnal Kewirausahaan dan Multi Talenta*, *2*(2), 138-147.

Alif, M. S., & Pratama, A. R. (2021). Analisis kesadaran keamanan di kalangan pengguna E-Wallet di Indonesia. *Automata*, *2*(1).

Hartanto, H., Rosadi, V., & Yosmar, E. A. (2023). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Wallet Dana. *PATTIMURA Legal Journal*, *2*(3), 267-279.