E-ISSN: 3031-8629
P-ISSN: 3032-3258
Halaman 15-27
Volume 1 Nomor 4 Tahun 2024

Menghadapi Ancaman Cyber : Strategi Keamanan Untuk Sistem Pembayaran E-Commerce

Titin sumarni[1], Eni Kurnia[2], Tiara Rahmadani[3], Rio Febrian Saven Saputra[4]

[1,2,3,4]Program Studi Ekonomi Syariah, Sekolah Tinggi Agama Islam Negeri (STAIN) Bengkalis

Email:Titinijal@gmail.com Kurniaeni780@gmail.com enazalina135@gmail.com riobkn28@gmail.com

Abstrak

Di era digital yang serba cepat ini, transaksi daring telah menjadi bagian integral dari kehidupan kita. Kemudahan dan kenyamanan berbelanja online telah mengubah cara kita berinteraksi dengan dunia. Namun, di balik kemudahan ini, terdapat ancaman laten yang mengintai - ancaman dunia maya. Sistem pembayaran e-commerce, yang menjadi tulang punggung transaksi daring, menjadi target empuk bagi para pelaku kejahatan siber. Selain teknologi, faktor manusia juga memainkan peran penting dalam menjaga keamanan sistem pembayaran e-commerce. Karyawan yang bertanggung jawab atas sistem pembayaran harus mendapatkan pelatihan yang memadai tentang keamanan siber dan praktik terbaik. Mereka harus menyadari ancaman yang ada dan mampu mengenali tanda-tanda serangan siber. Tujuan dari artikel ini adalah untuk mengetahui bagaimana cara Menghadapi Ancaman Cyber : Strategi Keamanan Untuk Sistem Pembayaran E-Commerce. Penyajian artikel ini, penulis menggunakan metode penelitian kualitatif, yaitu ditujukan untuk memahami fenomena-fenomena sosial dari sudut atau perspektif partisipan. Partisipan adalah orang-orang yang diakak berwawancara, diobservasi, diminta memberikan data, pendapat, pemikiran, persepsinya. Berdasarkan hasil pembahasan bahwa Keamanan adalah hal yang paling diutama setiap pelanggan dari bertransaksi di ecommerce. Keamanan dalam transaksi e-commerce sudah diatur

oleh pemerintah dalam undang – undang no. 11 tahun 2008, undang – undang no.8 tahun 1999, UU ITE dan adanya pihak kominfo yang mengawasi kegiatan e-commerce. Dalam bertransaksi kita tidak boleh lalai dan harus memperhatikan aspek – aspek penting, jika lalai kita bisa terkena penipuan dalam bertransaksi di e-commerce. Faktor – faktor terjadinya penipuan dalam transaksi ecommerce antara lain : pengetahuan yang minim, keborocan dara, tergiur pada hadiah palsu, tingginya tingkat pengangguran dan kemiskinan dan kebijakan keamanan pemerintah yang kurang tegas. Adapun bentuk dari penipuan dalam bertransaksi di e-commerce antara lain : phising, pharming, pretexting, quid pro quo dan menghubungi korban secara langsung.

Kata kunci: *E-Commerce, Cybercrime, Strategi Keamanan bertransaksi di E-Commerce*

Abstract

In this fast-paced digital era, online transactions have become an integral part of our lives. The ease and convenience of online shopping has changed the way we interact with the world. However, behind this convenience, there is a latent threat lurking - cyber threats. E-commerce payment systems, which are the backbone of online transactions, are easy targets for cybercriminals. Apart from technology, human factors also play an important role in maintaining the security of e-commerce payment systems. In presenting this article, the author uses qualitative research methods, which are aimed at understanding social phenomena from the participant's point of view or perspective. Participants are people who are interviewed, observed, asked to provide data, opinions, thoughts and perceptions. Based on the results of the discussion, security is the most important thing for every customer when making transactions in e-commerce. Security in e-commerce transactions has been regulated by the government in Law no. 11 of 2008, law no. 8 of 1999, the ITE Law and the existence of a Ministry of Communication and Information that supervises e-commerce activities. When making transactions, we must not be negligent and must pay attention to important aspects. If we are negligent, we could be exposed to

fraud in e-commerce transactions. Factors that cause fraud in e-commerce transactions include: minimal knowledge, waste of money, being tempted by fake gifts, high levels of unemployment and poverty and less strict government security policies. The forms of fraud in e-commerce transactions include: phishing, pharming, pretexting, quid pro quo and contacting the victim directly.

Keywords: *E-Commerce, Cybercrime, Security Strategy for transactions in E-Commerce*

PENDAHULUAN

Di era digital yang serba cepat ini, transaksi daring telah menjadi bagian integral dari kehidupan kita. Kemudahan dan kenyamanan berbelanja online telah mengubah cara kita berinteraksi dengan dunia. Namun, di balik kemudahan ini, terdapat ancaman laten yang mengintai - ancaman dunia maya. Sistem pembayaran e-commerce, yang menjadi tulang punggung transaksi daring, menjadi target empuk bagi para pelaku kejahatan siber.

Ancaman siber terhadap sistem pembayaran e-commerce bukan sekadar ancaman abstrak. Data menunjukkan bahwa serangan siber terhadap sistem pembayaran e-commerce meningkat secara signifikan dalam beberapa tahun terakhir. Peretas terus mengembangkan taktik dan strategi baru untuk mengeksploitasi kerentanan sistem dan mencuri informasi sensitif, seperti data kartu kredit, informasi pribadi, dan data keuangan. Dampaknya tidak hanya merugikan konsumen, tetapi juga dapat merusak reputasi dan kepercayaan terhadap bisnis e-commerce.

Untuk menghadapi ancaman siber yang semakin canggih, diperlukan strategi keamanan yang komprehensif dan proaktif. Sistem pembayaran e-commerce harus dirancang dengan mempertimbangkan aspek keamanan sebagai prioritas utama. Hal ini mencakup penggunaan teknologi enkripsi yang kuat, sistem autentikasi yang canggih, dan langkah-langkah pencegahan penipuan yang efektif.

Selain teknologi, faktor manusia juga memainkan peran penting dalam menjaga keamanan sistem pembayaran e-commerce. Karyawan yang bertanggung jawab atas sistem pembayaran harus mendapatkan pelatihan yang memadai tentang keamanan siber dan praktik terbaik. Mereka harus menyadari ancaman yang ada dan mampu mengenali tanda-tanda serangan siber.

Penting juga untuk membangun budaya kesadaran keamanan siber di seluruh organisasi. Konsumen juga harus dididik tentang praktik keamanan siber yang baik, seperti menggunakan kata sandi yang kuat, menghindari tautan mencurigakan, dan melaporkan aktivitas mencurigakan.

Kolaborasi antara pemerintah, industri, dan penegak hukum sangat penting dalam memerangi kejahatan siber. Pemerintah harus mengeluarkan peraturan dan kebijakan yang mendukung keamanan siber, sementara industri harus bekerja sama untuk berbagi informasi dan mengembangkan solusi keamanan yang lebih baik. Penegak hukum harus meningkatkan kemampuan mereka dalam menyelidiki dan menindak kejahatan siber.

Dengan menerapkan strategi keamanan yang komprehensif, meningkatkan kesadaran siber, dan bekerja sama secara aktif, kita dapat melindungi sistem pembayaran e-commerce dari ancaman siber dan memastikan bahwa transaksi daring tetap aman dan terpercaya.

METODE PENELITIAN

Penyajian artikel ini, penulis menggunakan metode penelitian kualitatif, yaitu ditujukan untuk memahami fenomena-fenomena sosial dari sudut atau perspektif partisipan. Partisipan adalah orang-orang yang diakak berwawancara, diobservasi, diminta memberikan data, pendapat, pemikiran, persepsinya.(Sandu Siyoto dan M. Ali Sodik 2015:42)

Teknik analisis data yang akan dilakukan oleh peneliti adalah teknik kualitatif dengan menggunakan model Milles dan Huberman. Aktivitas dalam analisa data antara lain sebagai berikut:(Sugiyono 2016:246–52)

1. *Data Reduction* (Reduksi Data)

Mereduksi data yaitu merangkum, memilih hal-hal yang pokok, memfokuskan pada hal-hal yang pokok, memfokuskan pada hal-hal yang penting, dicari tema dan polanya. Dengan demikian data yang telah direduksi akan memberikan gambaran yang lebih jalas dan mempermudah peneliti untuk melakukan pengumpulan data selanjutnya.

2. *Data Display* (Penyajian Data)

   Setelah data direduksi maka langkah selanjutnya adalah mendisplay data. Dalam penelitian kualitatif, penyajian data bisa diuraikan dalam uraian singkat, hubungan antar kategori dan sejenisnya, yang paling sering digunakan untuk penyajian data kualitatif dengan teks yang bersifat naratif. Dengan mendisplay data maka akan memudahkkan untuk memahami apa yang terjadi, merencanakan kerja selanjutnya berdasarkan apa yang dipahami.

3. *Conclusion Drawing* (Verifikasi)

   Langkah ketiga adalah penarikan kesimpulan dan verifikasi. Kesimpulan awal yang dikemukakan masih bersifat sementara, dan akan berubah bila tidak ditemukan bukti-bukti yang kuat yang mendukung pada tahap pengumpulan data berikutnya. Tetapi apabila kesimpulan yang dikemukakan pada tahap awal, didukung oleh bukti-bukti yang valid dan konsisten maka kesimpulan yang dikemukakan merupakan kesimpulan yang kredibel.

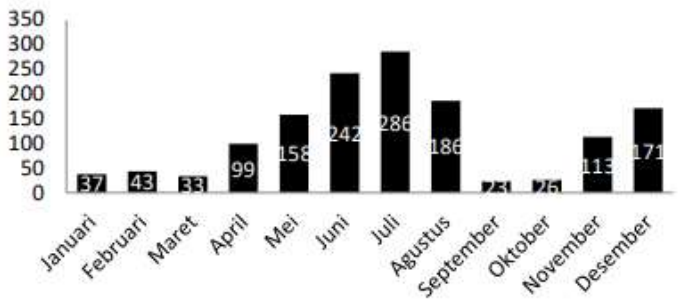
PEMBAHASAN

Electronic commerce (*E-commerce*) adalah aktivitas yang melibatkan transaksi jual beli oleh produsen dan konsumen dengan pemanfaatan teknologi digital yang diimplementasikan dalam kegiatan usaha melalui penggunaan internet. Tingginya akses pengguna online atau internet menjadi salah satu faktor semakin maraknya kasus ancaman *cyber*. Perkembangan teknologi secara tidak langsung mempengaruhi kemudahan penyebaran informasi dan data. Hal ini dapat meningkatkan risiko kejahatan dunia maya. Penanggulangan kejahatan dunia maya ini berdampak negatif, menyebabkan kerugian yang signifikan tidak hanya bagi perusahaan tetapi juga bagi pelanggannya. Hilangnya kepercayaan pengecer dan

pelanggan terhadap belanja online dianggap sebagai biaya yang tidak terlihat akibat kejahatan dunia maya.(Afzil Ramadian, Amanda Fitriyani, dan Neng Nanda Sarah Novita 2024:6)

Tim Pusat Kontak Siber BSSN selama tahun 2023 mendapatkan informasi sekitar 1.417 pengaduan *cyber*. Aduan dengan jumlah tertinggi terjadi pada bulan Juli dengan total 286 aduan, dapat dilihat pada grafik di bawah ini.

Gambar 2. Rekapitulasi Aduan *Cyber* 2023



Sumber : (BSSN, 2022)

Pengukuran i *e-commerce* itu dapat dilakukan melalui penilaian akan tingkat risiko yang tersedia serta mengimplementasikan strategi pengelolaan risiko. Adapun strategi pendekatan pada umumnya dilakukan dalam pengukuran manajemen risiko pada sebuah *e-commerce* , yaitu sebagai berikut:

1. Analisis Probabilitas-Dampak: Probabilitas dapat dinyatakan dalam persentase atau skala numerik lain yang menunjukkan kemungkinan terjadinya suatu risiko. Dampaknya dapat mencakup kerugian finansial, reputasi, atau operasional. Menggabungkan probabilitas dan dampak memberikan pemahaman yang dapat diandalkan tentang tingkat risiko secara keseluruhan.
2. Analisis Sensitivitas: Mengidentifikasi dan menganalisis faktor-faktor penting yang berkontribusi terhadap risiko bagi perusahaan e-commerce.

3. Metrik Kinerja : Metrik kinerja dapat mencakup jumlah insiden penipuan yang terdeteksi, waktu pemulihan dari serangan siber, tingkat kepatuhan terhadap peraturan, atau tingkat keberhasilan penerapan kebijakan keamanan. Dengan menggunakan metrik yang jelas, perusahaan dapat mengukur kemajuan manajemen risiko mereka dan menilai efektivitas strategi yang diterapkan.
4. Evaluasi Keuangan: Keuangan: Mengevaluasi dampak risiko terhadap kinerja keuangan perusahaan, antara lain: Contoh: hilangnya pendapatan, biaya pemulihan setelah serangan siber, kerugian akibat penipuan, dll. Penilaian ini membantu dalam memahami kontribusi risiko terhadap hasil keuangan perusahaan dan mendorong keputusan manajemen risiko yang cerdas.
5. Audit dan Evaluasi Eksternal: Pihak ketiga yang independen dapat dilibatkan untuk mengevaluasi kebijakan, prosedur, dan sistem manajemen risiko yang ada. Hasil audit atau penilaian eksternal ini memberikan gambaran obyektif mengenai efektivitas manajemen risiko pada perusahaan e-commerce.

Strategi pendekatan umumnya dapat digunakan untuk pengukuran risiko pada sebuah ecommerce. Strategi tersebut bervariasi tergantung kriteria, spesifikasi, ciri bisnis dan restrukturisasi organisasi. Pengukuran risiko *cybercrime* pada *e-commerce* merupakan proses yang dilakukan untuk mengidentifikasi, menganalisis, serta mengevaluasi potensi dari kerugian finansial dan reputasi yang dapat ditimbulkan oleh serangan cyber. Tujuannya yaitu untuk memahami tingkat risiko yang dihadapi bisnis dan mengambil langkah-langkah yang tepat untuk menguranginya.

Guna melakukan tindakan antisipatif untuk menanggulangi *cybercrime* tersebut, diperlukan *Cybersecurity* (keamanan siber) didefinisakan sebagai suatu proses yang dijalankan untuk mempertahankan dan mengurangi masalah privasi, keintegritasan serta terhadap adanya fakta yang tersedia. Proses tersebut dapat menjaga sistem informasi dari segala serangan fisik dan serangan *cyber*. *Cybersecurity* merujuk pada perlindungan terhadap informasi sesuai dengan jenis dan kepekaaan informasi yang ada dalam suatu organisasi untuk penggunaanya

secara strategis dalam. *Cybersecurity* dikatakan memegang peran cukup penting dalam melindungi bisnis e-commerce dari berbagai ancaman *cybercrime* yang semakin marak dan canggih. Beberapa hal penting mengenai peran dan pentingnya *cybersecurity* dalam *e-commerce* yaitu, *cybersecurity* melindungi aset berharga *e-commerce*, seperti data pelanggan, informasi keuangan, dan kekayaan intelektual, dari akses tidak sah, pencurian, atau kerusakan. *Cybersecurity* adalah sebagai perlindungan terhadap struktur cyber dari munculnya ancaman *cyber*. Oleh karena itu, *cybersecurity* bermanfaat cukup signifikan ketika melakukan perlindungan keamanan informasi maupun data dikarenakan perlu supaya melindungi informasi serta memberikan jaminan bahwa data yang dikirim dalam kondisi aman.

Faktor penyebab terjadinya penipuan dalam transaksi e-commerce:

Penipuan dalam transaksi *e-commerce* sudah sangat sering kita jumpai dimana pun, baik melalui social media, nomor handphone ataupun secara langsung. Biasanya penipu atau *cyber crime* akan berpura-pura mengaku dari pihak *e-commerce* resmi, lalu menwarkan hadiah palsu dengan iming-iming tertentu yang mengorbankan data pribadi korban bahkan hingga uang korban. *Cyber crime* sendiri biasanya memiliki trik untuk mengelabui korbannya. Namun sebenarnya apa saja faktor terjadinya penipuan dalam transaksi *e-commerve*. Berikut adalah faktor terjadinya penipuan dalam transaksi *e-commerce* berdasarkan study literature.

a. Faktor pengetahuan pengguna yang minim, Perlunya edukasi kepada seluruh masyarakat untuk mengetahui adanya ancaman penipu dari transaksi online. Mengingat di era digitalisasi ini, menuntut seluruh orang mau tak mau harus pandai menggunakan digital. Untuk itu, perlu adanya sosialisasi dan pemberitahuan kepada seluruh masyarakat untuk mengetahui adanya ancaman penipuan dalam transaksi digital.
b. Kebocoran data pengguna, Hal ini biasanya terjadi karena kesalahan kita sebagai pengguna. Yang perlu kita perhatikan akan data pribadi tidak bocor adalah, jangan pernah memberi data pribadi seperti : ktp, sim, nomor rekening, kode vertifikasi, dan data pribadi lainnya.

c. Pengguna tergiur dengan hadiah palsu, Segelintir orang ada sudah paham adanya penipuan dalam transaksi online, namun masih saja terjebak dengan kasus tersebut. Hal ini biasanya disebabkan oleh, tergiurnya pengguna oleh iming – iming hadiah puluhan juta rupiah ataupun barang mewah lainnya.
d. Tingginya angka pengangguran dan kemiskinan, Sempitnya lapangan kerja dan persaingan yang ketat membuat sebagaian orang berpikiran pendek untuk melakukan tindakan kejahatan. Dengan hanya bermodal kan janji palsu, para penipu transaksi online dapat melancarkan aksinya.
e. Sistem keamanan dan kurang tegasnya kebijakan pemerintah, Kasus kebocoran data pada aplikasi e-commerce Tokopedia, menunjukkan sistem keamanan e-commerce Indonesia yang tidak aman. Kurang tegasnya kebijakan pemerintah dalam hal ini, menjadikan kesempatan bagi para cyber crime.

Dalam melancarkan aksinya penipu online atau cyber crime memiliki beberapa teknik atau bentuk dalam mengambil data korban, berikut bentuk penipuan pada transaksi *e-commerce:*

1) Phising adalah aksi penipuan yang dilakukan dengan cara, *cyber crime* akan mengirimkan file melalui email yang berisi link palsu. *Cyber crime* akan mengelabui korban bahwa link tersebut adalah link resmi dari pihak *ecommerce*, sehingga korban harus mengisi data pribadi di link tersebut untuk mendapatkan hadiah yang di iming-imingkan. Teknik phising ini adalah Teknik yang paling banyak terjadi.
2) Pharming adalah aksi penipuan yang dilakukan cyber crime dengan cara mengelabui korban dengan mengarahkan ke situs web asli ke situs web palsu. Sehingga korba akan menyangka telah memasuki situs web asli dan tanpa ragu korban akan mengisi data pribadi atau data lainnya yang diminta oleh cyber crime melalui situs palsu.
3) Pretexting adalah aksi penipuan yang dilakukan cyber crime dengan cara meminta data pribadi korban dengan mengatas namakan e-commerce tertentu. Cyber crime akan mengaku, meminta data pribadi tersebut untuk keperlu korban

dalam mengakses e-commerce. Dengan begitu cyber crime akan mudah menggunakan data pribadi korban untuk kepentingan pribadinya.

4) Quid Pro Quo adalah aksi penipuan yang dilakukan cyber crime dengan mengiming – iming hadiah berupa uang tunai atau barang berharga lainnya dengan syarat terlebih dahulu korban harus memberi data pribadinya. Kemudian pelaku akan memanfaatkan data pribadi tersebut dan hadiah yang di imingimingkan akan diproses padahal hal itu tidak akan terjadi. karena cyber crime mengelabui korban untuk mendapatkan data pribadinya.
5) Menghubungi Korban, aksi ini adalah aksi yang paling dihindari karena aksi penipuan ini aksi yang paling banyak berhasil. Dengan cara cyber crime menelepon nomor telepon atau nomor whatsapp korban secara langsung, lalu mengaku berasal dari pihak e-commerce yang ingin memberikan hadiah dengan syarat hanya menyebutkan nomor rekening saja maka hadiah akan langsung masuk ke nomor rekening. Aksi ini adalah aksi yang paling sering berhasil, karena cyber crime akan berbicara seolah – olah seperti pihak e-commerce resmi, cyber crime menggunakan menggunakan bahasa baku layaknya layanan e-commerce pada umumnya.

Berikut beberapa langkah yang dapat diambil guna mencegah penipuan dalam bertransaksi : (Purnama Ramadani Silalahi dkk. 2022:233)

a) Pilih platform e-commerce yang resmi dan telah diawasi OJK
b) Perhatikan kode vertifikasi apakah sudah centang biru
c) Jangan membagikan kode vertifikasi yang bersifat rahasia
d) Wajib membaca secara teliti informasi dan proses transaksi
e) Slalu beritikad baik dalam melakukan transaksi
f) Membayar sesuia dengan nominal yang tercantum diaplikasi
g) Bijak dalam menanggapi kasus penipuan
h) Baca berita terkini tentang motif penipuan terbaru
i) Jangan langsung percaya dan tergiur oleh hadiah yang diberikan secara gratis
j) Slalu berhati – hati dalam melakukan transaksi

Kebijakan pemerintah terkait penipuan pada transaksi *e-commerce:*

UU NO. 11 Tahun 2008

Pada pasal 3 menjelaskan, pemanfaat teknologi informasi dan transaksis elektronik berdadarkan asas kepastian hukum. Pada pasal 28 dan 29 menjelaskan, setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan mengirimkan informasi yang berisi ancaman kekerasan yang ditujukkan secara pribadi. Kemudain berdasarkan 3 pasal tersebut ditindak lanjuti pada pasal 45 yaitu dipidana dengan pidana penjara paling lama 6 tahun atau denda satu miliar rupiah

UU No. 8 Tahun 1999

Pada pasal 44 menjelaskan, pemerintah mengakui Lembaga perlindungan kosumen swadaya untuk melakukan pengawasan pada masyarakat. Pada pasal 45 menjelaskan, setiap konsumen yang dirugiakan dapat menggugat tindakan yang terjadi. Kemudian pada pasal 62 menindak lanjuti para pelaku dengan pidana penjara paling lama 5 tahun ataupun denda dua miliar rupiah.

UU ITE

Pada pasal 4 menjelaskan, konsumen berhak mendapat informasi yang jelas, benar dan jujur apabila tidak sesuai konsumen berhak mendapat hak nya dan melakukan penuntutan. Selain itu pihak kominfo (kementerian komunikasi dan informatika) juga berhak dalam menangani kasus – kasu seperti pasal diatas. Kominfo berhak untuk menjaga kebocoran data masyarakat yang dimanfaatkan pihak tidak bertanggung jawab

KESIMPULAN

Electronic commerce (*E-commerce*) adalah aktivitas yang melibatkan transaksi jual beli oleh produsen dan konsumen dengan pemanfaatan teknologi digital yang diimplementasikan dalam kegiatan usaha melalui penggunaan internet. Tingginya akses pengguna online atau internet menjadi salah satu faktor semakin maraknya kasus ancaman *cyber*. Perkembangan teknologi secara tidak langsung mempengaruhi kemudahan penyebaran informasi dan data. Hal ini dapat

meningkatkan risiko kejahatan dunia maya. Penanggulangan kejahatan dunia maya ini berdampak negatif, menyebabkan kerugian yang signifikan tidak hanya bagi perusahaan tetapi juga bagi pelanggannya.

Guna melakukan tindakan antisipatif untuk menanggulangi *cybercrime* tersebut, diperlukan *Cybersecurity* (keamanan siber) didefinisakan sebagai suatu proses yang dijalankan untuk mempertahankan dan mengurangi masalah privasi, keintegritasan serta terhadap adanya fakta yang tersedia. Proses tersebut dapat menjaga sistem informasi dari segala serangan fisik dan serangan *cyber.*

Keamanan adalah hal yang paling diutama setiap pelanggan dari bertransaksi di ecommerce. Keamanan dalam transaksi e-commerce sudah diatur oleh pemerintah dalam undang – undang no. 11 tahun 2008, undang – undang no.8 tahun 1999, UU ITE dan adanya pihak kominfo yang mengawasi kegiatan e-commerce. Dalam bertransaksi kita tidak boleh lalai dan harus memperhatikan aspek – aspek penting, jika lalai kita bisa terkena penipuan dalam bertransaksi di e-commerce. Faktor – faktor terjadinya penipuan dalam transaksi ecommerce antara lain : pengetahuan yang minim, keborocan data, tergiur pada hadiah palsu, tingginya tingkat pengangguran dan kemiskinan dan kebijakan keamanan pemerintah yang kurang tegas. Adapun bentuk dari penipuan dalam bertransaksi di e-commerce antara lain : phising, pharming, pretexting, quid pro quo dan menghubungi korban secara langsung.

DAFTAR PUSTAKA

Afzil Ramadian, Amanda Fitriyani, dan Neng Nanda Sarah Novita. 2024. “MENGUKUR DAN MENGELOLA RISIKO CYBERCRIME DALAM E-COMMERCE: PERAN STRATEGIS CYBERSECURITY UNTUK KEAMANAN INFORMASI DAN PERLINDUNGAN DATA.” *Edunomika* Vol. 08 No. 02:6.

Purnama Ramadani Silalahi, Aisy Salwa Daulay, Tanta Sudiro Siregar, dan Aldy Ridwan. 2022. “Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online.” *Profit: Jurnal Manajemen, Bisnis dan Akuntansi* Vol.1, No.4.

Sandu Siyoto dan M. Ali Sodik. 2015. *Dasar Metodologi Penelitian*. Yogyakarta: Literasi Media Publishing.

Sugiyono. 2016. *Metode Penelitian Kuantitatif, Kualitatif Dan R&D*. Bandung: ALFABETA.

Siregar, Alya Rahmayani, Azrai Harahap, and Mahardhika Sastra Nasution. "Etika Komunikasi Media Digital Di Era Post-Truth." Jurnal Paradigma: Jurnal Multidisipliner Mahasiswa Pascasarjana Indonesia 5, no. 1 (2024): 39–53.

Sugiyono. Metode Penelitian Kombinasi (Mixed Methods). Bandung: CV. Alfabeta, 2018.

Suryani, Tatik, Abu Amar Fauzi, and Mochamad Nurhadi. "Enhancing Brand Image in the Digital Era : Evidence from Small and Medium-Sized Enterprises (SMEs) in Indonesia." Gadjah Mada International Journal of Business 23, no. 3 (2021): 314–340.

Sutama, Gede Rai, and Putu Aditya Pratama. "Efektivitas Sosial Media Sebagai Media Pemasaran Digital." Jurnal Komputer dan Teknologi Sains (KOMTEKS) 2, no. 1 (2023): 8–11.

Wachyudi, Sudiana, Annisaa Eka Warliati, Jasmine Callysta Setiawan, Alamat Jalan, Perjuangan No, Kota Cirebon, and Jawa Barat. "Strategi Promosi Berbasis Branding , Advertising , Selling (BAS) Dalam Industri Pariwista Kecamatan Talun Kabupaten Cirebon." Global Leadership Organizational Research in Management 2, no. 3 (2024): 302.