Jurnal Bersama Ilmu Ekonomi
https://jurnal.literasisains.id/index.php/EKONOM
e-ISSN 3090-6393 | p-ISSN 3090-6407
Vol. 2 No. 1 (Februari 2026) 57-65
DOI: 10.55123/ekonom.v2i1.448

Analisis Risiko Keamanan Siber pada Aplikasi Belanja Online dengan Fitur Promo dan Diskon

Rizka Fitri Amalia[1], Khoerul Maliyah[2], Aulia 'Annafisah[3], Najwa Tsania[4], Ardine Arundati[5]
[1,2,3,4,5]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Walisongo, Kota Semarang, Indonesia
Email: [1]riskafitri604@gmail.com, [2]maliyahkhoerul129@gmail.com, [3]auliaannafisa@gmail.com, [4]nawtsa23@gmail.com, [5]secounda980@gmail.com

Informasi Artikel
Submitted : 22-12-2025
Accepted : 06-01-2026
Published : 15-02-2026

Keywords:
Cybersecurity
E-commerce
Promotions and Discounts
Cyber Risk
Personal Data

Abstract

The rapid development of e-commerce has driven the increasing use of online shopping apps with various promotional and discount features as digital marketing strategies. While these features are effective in increasing purchase interest and transaction volume, their presence also has the potential to increase cybersecurity risks, especially during major promotional periods. Threats such as phishing, personal data theft, account hacking, and voucher manipulation often exploit users' impulsive behavior focused on price advantages. This study aims to explore users' experiences, perceptions, and responses to cybersecurity risks that arise when using promotional and discount features in online shopping apps, as well as to identify the types of threats and their triggers. This study used a descriptive qualitative method with a phenomenological approach. Data were obtained through case documentation, digital security incident reports, and a review of literature relevant to cybersecurity and e-commerce. Data analysis was conducted through data reduction, grouping themes, and interpreting phenomena based on user experiences. The results show that cybersecurity risks increase significantly during major promotional periods due to high user traffic and low consumer vigilance. Promotional and discount features are often exploited by cybercriminals through fake links, fictitious pop-ups, and voucher redirects, resulting in losses such as lost account access and unauthorized transactions. This study concludes that cybersecurity in online shopping applications depends not only on technological systems but also on user behavior and security literacy. Therefore, an integrated mitigation strategy is needed through strengthening application security systems and improving digital security education for users.

Abstrak

Perkembangan pesat e-commerce mendorong meningkatnya penggunaan aplikasi belanja online dengan berbagai fitur promosi dan diskon sebagai strategi pemasaran digital. Meskipun fitur tersebut efektif meningkatkan minat beli dan volume transaksi, keberadaannya juga berpotensi meningkatkan risiko keamanan siber, terutama selama periode promo besar. Ancaman seperti phishing, pencurian data pribadi, peretasan akun, dan manipulasi voucher kerap memanfaatkan perilaku impulsif pengguna yang berfokus pada keuntungan harga. Penelitian ini bertujuan untuk mengeksplorasi pengalaman, persepsi, dan respons pengguna terhadap risiko keamanan siber yang muncul saat menggunakan fitur promo dan diskon pada aplikasi belanja online, serta mengidentifikasi bentuk ancaman dan faktor pemicunya. Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan fenomenologis. Data diperoleh melalui dokumentasi kasus, laporan insiden keamanan digital, serta kajian literatur yang relevan dengan topik keamanan siber dan e-commerce. Analisis data dilakukan melalui proses reduksi data, pengelompokan tema, dan interpretasi fenomena berdasarkan pengalaman pengguna. Hasil penelitian menunjukkan bahwa risiko keamanan siber meningkat secara signifikan selama periode promo besar akibat tingginya lalu lintas pengguna dan rendahnya kewaspadaan konsumen. Fitur promo dan diskon sering dimanfaatkan pelaku kejahatan siber melalui tautan palsu, pop-up fiktif, dan pengalihan voucher, yang menyebabkan kerugian berupa kehilangan akses akun dan transaksi tidak sah. Penelitian ini menyimpulkan bahwa keamanan siber pada aplikasi belanja online tidak hanya bergantung pada sistem teknologi, tetapi juga pada perilaku dan literasi keamanan pengguna. Oleh karena itu, diperlukan strategi mitigasi yang terintegrasi melalui penguatan sistem keamanan aplikasi serta peningkatan edukasi keamanan digital bagi pengguna.

Kata Kunci: Keamanan Siber, E-commerce, Promo dan Diskon, Risiko Cyber, Data Pribadi.

1. PENDAHULUAN

Pertumbuhan pesat e-commerce dalam beberapa tahun terakhir telah mendorong perubahan signifikan dalam perilaku konsumen, khususnya dalam aktivitas belanja online yang kini semakin bergantung pada sistem digital. Dalam konteks ini, keamanan siber menjadi fondasi utama yang menentukan keberlangsungan dan keandalan platform belanja online. Seiring dengan meningkatnya frekuensi penggunaan aplikasi belanja, ancaman siber seperti pencurian data pribadi, serangan malware, manipulasi transaksi, hingga penipuan berbasis rekayasa sosial juga mengalami peningkatan yang signifikan (Agung Wijoyo et al. 2024). Kondisi ini menunjukkan bahwa perkembangan teknologi digital tidak hanya menghadirkan kemudahan, tetapi juga memperbesar risiko yang dihadapi oleh pengguna.

Penelitian sebelumnya mengungkapkan bahwa tantangan dalam melindungi data pribadi pengguna semakin kompleks, terutama karena konsumen cenderung membagikan informasi sensitif seperti data identitas, nomor telepon, alamat, hingga informasi keuangan selama proses transaksi online (Poeja Kehista et al., 2023). Peningkatan volume dan variasi data yang diproses oleh aplikasi belanja memperluas potensi terjadinya kebocoran data, baik akibat kelemahan sistem internal maupun keterlibatan pihak ketiga dalam ekosistem digital. Selain itu, studi selama lima tahun terakhir menunjukkan bahwa fitur promo dan diskon yang dirancang untuk meningkatkan daya tarik konsumen justru sering dimanfaatkan sebagai celah oleh pelaku kejahatan siber. Promo palsu, tautan diskon fiktif, serta pesan penawaran yang meniru tampilan resmi aplikasi kerap digunakan untuk mengarahkan pengguna ke serangan phishing atau malware (Iskandar et al., 2024). Oleh karena itu, isu keamanan siber dalam aplikasi belanja online tidak lagi dapat dipandang semata-mata sebagai persoalan teknis, melainkan juga berkaitan erat dengan kepercayaan dan persepsi pengguna terhadap platform digital.

Kerentanan sistem aplikasi belanja online semakin meningkat seiring dengan penambahan berbagai fitur tambahan yang bertujuan meningkatkan pengalaman pengguna. Integrasi sistem pembayaran digital, fitur dompet elektronik, gamifikasi promo, hingga notifikasi diskon real-time memang memberikan nilai tambah dari sisi pemasaran, namun di sisi lain berpotensi memperluas titik serangan siber (Aji et al., 2023). Setiap fitur baru membawa kompleksitas teknis yang menuntut pengelolaan keamanan yang lebih ketat. Beberapa penelitian mencatat bahwa pada periode diskon besar-besaran seperti kampanye harbolnas atau flash sale, lonjakan lalu lintas pengguna terjadi secara drastis. Situasi ini membuka peluang terjadinya serangan distributed denial of service (DDoS), kegagalan sistem, serta penipuan transaksi akibat lemahnya proses verifikasi (Tamzil & Deby Aprilia Ningrum, 2022).

Selain risiko teknis, aspek privasi pengguna juga menjadi isu krusial. Data pengguna tidak hanya diproses oleh satu sistem, tetapi sering kali melibatkan berbagai layanan pihak ketiga seperti penyedia pembayaran, logistik, dan analitik pemasaran. Kondisi ini meningkatkan potensi kebocoran data dari berbagai arah, baik disengaja maupun tidak disengaja (Poeja Kehista et al., 2023). Namun, penelitian terbaru menunjukkan bahwa sebagian besar pengguna belum memiliki kesadaran yang memadai terhadap risiko keamanan siber tersebut. Fokus utama konsumen masih tertuju pada besarnya promo dan rendahnya harga, sehingga aspek keamanan sering kali diabaikan dalam proses pengambilan keputusan pembelian (Mendrofa et al. 2021). Hal ini mengindikasikan adanya kesenjangan antara tingkat risiko aktual dengan persepsi risiko pengguna.

Meskipun berbagai studi telah mengkaji keamanan dalam konteks e-commerce secara umum, masih relatif sedikit penelitian yang secara spesifik menganalisis keterkaitan antara fitur promo dan diskon dengan peningkatan risiko ancaman siber. Padahal, fitur promo sering kali mendorong perilaku pembelian impulsif, yang membuat pengguna kurang waspada terhadap potensi penipuan. Pelaku kejahatan siber memanfaatkan kondisi ini melalui berbagai modus, seperti tautan promosi

palsu, pop-up diskon fiktif, manipulasi voucher, hingga penyamaran akun resmi aplikasi (Agung Wijoyo et al. 2024). Fenomena ini menunjukkan adanya celah penelitian yang belum dieksplorasi secara mendalam dalam studi sebelumnya.

Selain itu, sebagian penelitian terdahulu cenderung berfokus pada keamanan proses transaksi secara teknis, tanpa mengaitkannya dengan pola kampanye diskon yang memicu lonjakan lalu lintas pengguna dan menciptakan kerentanan sistem baru, seperti beban server yang berlebihan atau kegagalan verifikasi kode promo (Mendrofa et al, 2021). Padahal, interaksi pengguna dengan fitur diskon merupakan elemen krusial dalam strategi pemasaran aplikasi belanja online yang memiliki implikasi langsung terhadap keamanan siber. Oleh karena itu, diperlukan pendekatan analisis risiko yang lebih komprehensif dan kontekstual.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengeksplorasi pengalaman, persepsi, dan respons pengguna terhadap risiko keamanan siber yang muncul saat menggunakan fitur promo dan diskon dalam aplikasi belanja online. Penelitian ini juga berupaya mengidentifikasi jenis ancaman siber yang paling sering terjadi serta faktor-faktor yang memicu munculnya risiko tersebut dari sudut pandang pengguna. Selain itu, penelitian ini bertujuan untuk merumuskan rekomendasi strategi peningkatan keamanan yang berorientasi pada pengalaman pengguna, sehingga dapat membantu platform e-commerce dalam merancang fitur promo yang tidak hanya menarik secara komersial, tetapi juga aman secara digital. Dengan demikian, penelitian ini diharapkan mampu mengisi celah penelitian sebelumnya dan memberikan kontribusi teoritis maupun praktis dalam pengembangan keamanan siber pada aplikasi belanja online berbasis fitur promo dan diskon.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan fenomenologis untuk mengkaji pengalaman, persepsi, dan respons pengguna terhadap risiko keamanan siber dalam penggunaan fitur promo dan diskon pada aplikasi belanja online. Pendekatan kualitatif dipilih karena penelitian ini berfokus pada pemahaman mendalam terhadap makna yang dibangun pengguna berdasarkan pengalaman langsung mereka saat berinteraksi dengan sistem digital, khususnya dalam konteks ancaman siber yang tidak selalu disadari secara teknis oleh pengguna (Noor, 2020). Metode ini memungkinkan peneliti menggambarkan fenomena secara kontekstual sesuai dengan realitas yang dialami oleh subjek penelitian.

Pendekatan fenomenologis digunakan untuk menangkap pengalaman hidup (lived experiences) pengguna ketika menghadapi potensi risiko keamanan siber selama mengakses promo dan diskon. Pendekatan ini menekankan pada cara individu memaknai suatu peristiwa berdasarkan pengalaman subjektif mereka, termasuk bagaimana pengguna menyadari ancaman, mengambil keputusan, serta merespons insiden keamanan digital. Fenomenologi dipandang relevan karena risiko keamanan siber dalam e-commerce tidak hanya dipengaruhi oleh sistem teknologi, tetapi juga oleh persepsi, emosi, dan perilaku impulsif pengguna dalam merespons penawaran promosi (Alharbi & Drew, 2020).

Sumber data dalam penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh melalui dokumentasi pengalaman pengguna yang bersumber dari laporan insiden keamanan siber, pengaduan konsumen, serta ulasan pengguna pada platform belanja online yang berkaitan dengan penggunaan fitur promo dan diskon. Data ini mencerminkan kejadian nyata yang dialami pengguna, seperti penerimaan tautan promo palsu, gangguan akses akun, serta transaksi tidak sah. Data sekunder diperoleh dari jurnal ilmiah, buku akademik, dan laporan resmi lembaga keamanan digital yang membahas isu keamanan siber, e-commerce, dan perlindungan data pribadi sebagai landasan teoritis penelitian (Nirwana et al., 2024).

Pengumpulan data dilakukan melalui metode dokumentasi, pengamatan non-partisipatif, dan tinjauan literatur. Metode dokumentasi digunakan untuk menghimpun data berupa laporan insiden keamanan, arsip pengaduan pengguna, serta catatan resmi terkait kasus penipuan digital pada aplikasi belanja online. Pengamatan non-partisipatif dilakukan dengan menganalisis pola kemunculan promo palsu, tautan phishing, dan notifikasi diskon mencurigakan tanpa keterlibatan langsung peneliti dalam aktivitas pengguna. Pendekatan ini memungkinkan peneliti mengidentifikasi pola ancaman siber yang muncul bersamaan dengan kampanye promosi digital (Iskandar, 2024).

Analisis data dilakukan melalui tahapan analisis fenomenologis yang meliputi bracketing, reduksi data, pengelompokan tema, dan interpretasi makna esensial. Tahap bracketing dilakukan dengan menangguhkan asumsi peneliti agar interpretasi tetap berfokus pada pengalaman pengguna. Selanjutnya, data direduksi dengan menyaring informasi yang relevan dengan tujuan penelitian. Data yang telah diseleksi kemudian dikodekan dan dikelompokkan ke dalam tema-tema utama, seperti bentuk ancaman siber, faktor pemicu risiko, dan respons pengguna terhadap insiden keamanan. Proses analisis ini mengacu pada model analisis data kualitatif interaktif yang menekankan keterkaitan antara data dan interpretasi makna.

Untuk menjaga keabsahan temuan, penelitian ini menerapkan triangulasi sumber dengan membandingkan data dokumentasi, hasil pengamatan, dan temuan dari literatur ilmiah. Pendekatan ini digunakan untuk memastikan konsistensi dan kredibilitas hasil analisis, sehingga kesimpulan yang dihasilkan dapat dipertanggungjawabkan secara akademik dan relevan dengan konteks penelitian keamanan siber pada aplikasi belanja online (Wijoyo et al., 2024).

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Berdasarkan studi awal tentang laporan insiden keamanan e-commerce di Indonesia selama periode 2022-2024, terungkap bahwa peningkatan penipuan phishing dan pencurian data pengguna sering terjadi selama acara promo besar seperti Harbolnas dan flash sale (KominfoCSIRT, 2024). Catatan dari berbagai platform belanja online menunjukkan bahwa sejumlah pengguna menjadi korban penipuan melalui tautan promo palsu yang dikirim melalui pesan teks saat mereka mencari diskon. Ulasan pengguna mengungkapkan keluhan tentang pop-up palsu, masalah login akun, dan pembatalan transaksi setelah memasukkan voucher tertentu, yang menunjukkan kemungkinan manipulasi sistem. Selain itu, dokumen dari lembaga keamanan digital mencatat peningkatan taktik rekayasa sosial yang menargetkan pengguna yang tertarik dengan voucher pengiriman gratis. Secara keseluruhan, hasil studi awal ini menjelaskan bahwa aktivitas promo dan diskon dimanfaatkan oleh pelaku kejahatan sebagai kesempatan untuk menipu pengguna.

3.2 Pembahasan

3.2.1 Analisis Pengalaman, Persepsi, dan Respons Pengguna terhadap Risiko Keamanan Siber

Analisis ringkasan dari wawancara pengguna menunjukkan bahwa risiko keamanan paling sering terjadi ketika pengguna menerima tautan promo dari sumber yang tidak terpercaya atau ketika mereka terburu-buru mengakses penawaran diskon tertentu. Hal ini biasanya terjadi selama periode promo besar seperti 11.11 atau 12.12, ketika pengguna merasa harus bertindak cepat untuk mendapatkan harga terbaik. Korban umumnya adalah mereka yang tidak terbiasa memverifikasi keaslian tautan atau tidak mengenali tanda-tanda situs web palsu. Respons pengguna terhadap situasi ini sangat bervariasi; sebagian langsung memblokir pesan mencurigakan, sementara yang lain membuka tautan karena tampak meyakinkan. Saat serangan terjadi, pengguna sering melaporkan kehilangan akses ke akun mereka, perubahan kata sandi otomatis, atau pengurangan saldo tanpa izin.

Analisis lebih lanjut menunjukkan bahwa moivasi utama mereka untuk terus berbelanja adalah fokus pada diskon dan manfaat finansial, yang mengurangi kesadaran mereka akan keamanan. Pengalaman seperti kesulitan masuk ke akun, transaksi yang gagal, dan pop-up palsu telah membuat beberapa pengguna enggan melanjutkan berbelanja selama periode promo. Pengguna juga menyatakan bahwa notifikasi promosi yang berlebihan seringkali membuat mereka kesulitan membedakan antara notifikasi asli dan palsu. Dalam beberapa kasus, pengguna mengambil langkah pencegahan seperti mengganti kata sandi dan mengaktifkan otentikasi dua faktor, meskipun tidak semua memahami cara meningkatkan keamanan akun. Oleh karena itu, persepsi dan respons pengguna menunjukkan bahwa fitur promo tidak hanya meningkatkan minat belanja saja tetapi juga memperbesar risiko keamanan potensial.

Temuan dari pengalaman pengguna konsisten dengan laporan keamanan digital yang menyatakan bahwa tindakan implusif dalam mengejar promo dan diskon merupakan penyebab utama serangan phishing yang berhasil pada platform *e-commerce* (Kominfo-CSIRT, 2024). Temuan ini memperkuat hasil penelitian (Kehista et al., 2023), yang mengungkapkan bahwa konsumen sering mengabaikan pemeriksaan keamanan selama periode promo aktif. Sebaliknya, temuan ini mengonfirmasi pandangan dari (Mendrofa et al., 2025) bahwa program diskon meningkatkan risiko di lingkungan digital akibat beban sistem yang berat dan volume transaksi yang tinggi. Namun, studi ini memberikan kontribusi baru melalui deskripsi rinci tentang pengalaman langsung pengguna dalam berinteraksi dengan fitur promo, yang belum banyak dieksplorasi dalam studi sebelumnya. Secara umum, interpretasi pengalaman penguna menunjukkan bahwa keamanan siber tidak hanya bergantung pada teknologi sistem, tetapi juga pada tindakan dan kesadaran konsumen.

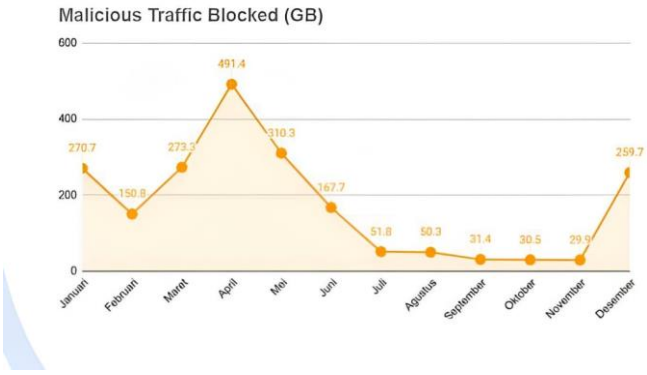
3.2.2 Analisis Bentuk Ancaman, Faktor Penyebab, dan Rekomendasi Strategi Mitigasi

Analisis data dokumentasi dan laporan insiden menunjukkan bahwa ancaman yang paling sering terjadi meliputi phishing melalui tautan promo, peretasan akun menggunakan metode credential stuffing, dan pengalihan voucher yang mengarahkan pengguna ke halaman pembayaran palsu. Ancaman-ancaman ini umumnya paling intensif pada malam hari atau selama periode flash sale, ketika sistem mengalmai beban lalu lintas yang berlebihan pelaku kejahatan memanfaatkan obsesi pengguna terhadap harga rendah, sehingga mereka dengan mudah diarahkan ke situs palsu tanpa memperhatikan aspek keamanan. Selain itu, kerentanan sistem muncul ketika aplikasi menangani sejumlah besar permintaan kode promo secara bersamaan, memungkinkan peretas memanfaatkan celah teknis seperti batas kecepatan yang lemah. Analisis mendalam juga mengidentifikasi pola pesan promo palsu yang didistribusikan melalui WhatsApp dan Telegram yang menyerupai pemberitahuan resmi dari aplikasi belanja online tersebut. Faktor risiko lainnya diicu oleh pemahaman pengguna yang terbatas tentang perlindungan akun dan kurangnya pendidikan keamanan di halman promo aplikasi. Beberapa insiden menunjukkan bahwa pengguna sering secara tomatis menyimpan informasi keratu pembayaran tanpa lapisan keamanan tambahan, sehingga memudahkan transaksi ilegal saat akun diretas. Selain itu, frekuensi tinggo notifikasi promo membuat pengguna kesulitan membedakan antara informasi yang sah dan penipuan. Dari pola-pola ini, jelas bahwa ancaman tidak hanya berasal dari aspek teknis, tetapi juga dipengaruhi oleh aspek psikologis dan kebiasaan pengguna. Oleh karena itu, menganalisis faktor-faktor ini sangat penting untuk menentukan strategi mitigasi yang paling tepat digunakan.

Temuan ini sejalan dengan penelitian (Agung Wijoyo et al, 2024), yang menjelaskan bahwa risiko terhadap sistem infromasi meningkat sering penambahan fitur pada aplikasi, seperti notifikasi, integrasi pembayaran, dan layanan pihak ketiga. Hasil penelitian ini juga memperkuat kesimpulan (Mendrofa et al. 2021) bahwa perode ini meningkatkan kemungkinan serangan akibat beban sistem yang tinggi dan paparan penggunaan yang luas. Namun, penelitian ini memberikan kontribusi baru dengan mengidentifikasi pola ancaman spesifikasi yang muncul pada fitur promo dan diskon,

terutama yang terkait dengan promo palsu yang belum banyak dibahas dalam penelitian sebelumnya. Rekomendasi mitigasi yang dihasilkan termasuk penguatan ptentikasi, penyaringan notifikasi, dan penyediaan pendidikan keamanan pada halaman promo sesuai dengan temuan Ningrum (Tamzil & Deby Aprilia Ningrum, 2022), mengenai kebutuhan untuk memperkuat kontrol keamanan pada aplikasi belanja online. Oleh karena itu, pembhasan ini menunjukkan bahwa pendekatan mitigasi perlu mengintegrasikan elmen teknis aplikasi dengan perilaku pengguna.

3.2.3 Gambar dan Illustrasi



Gambar 1. Trafik Anomali Periode Januari-Desember 2024

Grafik tersebut menggambarkan fluktuasi volume lalu lintas berbahaya yang berhasil dicegah selama satu tahun penuh. Secara keseluruhan, pola tersebut tampak tidak stabil, dengan puncak yang mencolok pada April mencapai 491,4 GB, menandakan peningkatan tajam tingkat ancaman selama periode tersebut, jumlah serangan secara bertahap menurun hingga mencapai titik terendah antara September dan November, berkisar antara 30 hingga 31 GB. Namun, volume kembali melonjak pada Desember hingga 259,7 GB, yang mungkin mencerminkan peningkatan aktivitas siber menjelang akhir tahun. Variasi semacam ini menunjukkan bahwa tingkat ancaman siber cenderung bersifat musiman, sehingga memerlukan pemantauan terus menerus untuk memastikan bahwa langkah-langkah pencegahan aktif.

Key	Category	Blocked
	DDoS Reputation	**61.1 GB**
	Location Based Threats	**1.9 GB**
	Command and Control	**390.0 MB**
	Mobile	**21.7 MB**
	Malware	**17.2 MB**

Gambar 2. Top 5 Trafik Anomali

Tabel ini menunjukkan berbagai kategori ancaman siber yang berhasil dicegah, beserta jumlah data yang terlibat. Ancaman terbesar berasal dari DdoS reputation, dengan volume 61,1 GB, mencerminkan upaya intensif untuk melampaui kapasitas sistem melalui banjir lalu lintas. Selanjutnya, ancaman berbasis lokasi tercatat sebesar 1,9 GB, menunjukkan aktivitas akses mencurigakan dari lokasi geografis tertentu. Kategori perintah dan kontrol mencapai 309 MB, menunjukkan upaya untuk berkomunikasi dengan server utama yang biasanya digunakan untuk

mengoperasikan atau mengendalikan perangkat yang terinfeksi. Ancaman yang berasal dari perangkat seluler dan malware menunjukkan volume yang lebih kecil, masing-masing 31,7 MB dan 17,2 MB, tetapi tetap memerlukan kewaspadaaan karena dapat menjadi titik masuk untuk serangan di masa depan. Secara keseluruhan, data ini menegaskan bahwa berbagai jenis ancaman siber tetap aktif dan memerlukan sistem deteksi dan pencegahan yang komprehensif untuk pengelolaan yang efektif.

4. KESIMPULAN

Penelitian ini membuktikan bahwa peningkatan risiko keamanan siber erat kaitannya dengan fitur promosi dan diskon pada aplikasi belanja online. Hal ini terutama disebabkan oleh kecenderungan pengguna untuk bertindak impulsif, volume lalu lintas yang tinggi selama periode diskon, dan kurangnya literasi keamanan. Analisis pengalaman dan persepsi pengguna menunjukkan bahwa ancaman seperti phishing, pengalihan voucher, serangan credential stuffing, dan pop-up palsu sering muncul ketika pengguna mengakses tautan promosi dari sumber yang tidak terverifikasi. Faktor utama yang memicu hal ini meliputi beban sistem yang berat, desain notifikasi yang berlebihan, dan pendidikan keamanan yang minim dari platform. Studi ini juga mengidentifikasi bahwa interaksi pengguna dengan fitur promosi tidak hanya membuka pintu bagi serangan teknis tetapi juga menimbulkan risiko psikologis yang membuat pengguna lebih cenderung mengabaikan prosedur keamanan dasar. Berdasarkan temuan ini, studi ini merekomendasikan penguatan otentikasi, penyaringan, dan verifikasi notifikasi promosi, serta penyediaan pendidikan keamanan yang lebih eksplisit di halaman diskon. Untuk penelitian di masa depan, para peneliti menyarankan untuk melakukan pengujian teknis langsung terhadap kerentanan sistem promosi, serta studi perbandingan antara berbagai platform untuk memetakan pola ancaman secara lebih luas.

DAFTAR PUSTAKA

Agustin, S. (2024). Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber. *JURNAL PENELITIAN MULTIDISIPLIN BANGSA*. 1(6), 500-504.

Ahmad, S. (2019). Menelisik Ketegasan Hukum Keluarga Islam di Pakistan. *Al-Mashlahah*, *15*(1), 87–97. http://jurnaliainpontianak.or.id/index.php/Almaslahah /article/view/1386

Ahmad, S. (2020). *Transformasi Hukum Pembuktian Perkawinan dalam Islam*. Airlangga University Press. https://books.google.co.id/books?hl=id&lr=&id=v QvyDwAA QBAJ&oi=fnd&pg=PP1&ots=ctXRKXFDi&sig=V9F3_1JOuRwhc2tdGDt-pvPaoCE&redir_esc=y#v=onepage&q&f=false

Aji, M. G. B., Mustofa, M. H. Al, Saputra, R., & Wardani, S. N. (2023). Analis Resiko Keamanan Pada E-commerce Shopee Terhadap Kenyamaan Konsumen Menggunakan Metode Kualitatif. *Prosiding Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB)*, 79–83.

Asiyanti, A. P. D., & Agussalim. (2024). Strategi Manajemen Risiko dan Keamanan Siber dalam Ekonomi Digital: Tinjauan Literatur. *Jurnal Penelitian Sistem Informasi*. 2(4), 90-110. DOI : https://doi.org/10.54066/jpsi.v2i4.2562

Assegaf, Ahmad. (2020). Strategi Kolaborasi BAZNAS FEBI dalam aktivitas kewirausahaan. *Al-Mashlahah*, *15*(1), 87–97. https://doi.org/10.37706/iconz.2019.161

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Farahdiya, A .T.,Mulyana, S. L., & Asri, T. P. (2025). IMPLEMENTASI CYBER SECURITY DALAM SISTEM TRANSAKSI KEUANGAN DIGITAL. *Jurnal Ilmu Ekonomi Manajemen Bisnis dan Akuntansi*. 2(4), 276-289. DOI : https://doi.org/10.61722/jemba.v2i4.1157

Fujiama Diapoldo Silalahi. (2022). *KEAMANAN SIBER (Cyber Security)*. Yayasan Prima Agus Teknik dengan Universitas STEKOM.

Hafizuddin, F. A.,& Sugiantoro, B. (2024). Evaluasi Keamanan Sistem Informasi Pada Penyedia Layanan Cloud Dan Perlindungan Data Pribadi Berdasarkan Index Kami Versi 4.2 (Studi Kasus : PTIPD UIN Sunan Kalijaga Yogyakarta). *CyberSecurity dan Forensik Digital*. 7(1), 7-17.

Hayrani. (2021). *Pengaruh Persepsi Resiko, Keamanan, Kemudahan Penggunaan Aplikasi, Promosi Flash Sale Terhadap Kepuasan Konsumen Di Situs Jual Beli Online Shopee*. Universitas Lampung.

Iskandar, O. (2024). Analisis kejahatan online phishing pada masyarakat. *Leuser: Jurnal Hukum Nusantara*, *1*(2), 32–36.

Kedua, T. W. Z., & Zebua, J. A. (2024). ANALISIS KEAMANAN SISTEM INFORMASI PADA PERUSAHAAN E-COMMERCE DI INDONESIA. *IDENTIK: Jurnal Ilmu Ekonomi, Pendidikan Dan Teknik*, *01*(03), 68–75.

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625–632.

Kominfo-CSIRT. (2024). *LAPOR AN TAHUNAN KOMINFO-CSIRT*. csirt.komdigi.go.id

Mendrofa, M. S. D., Waruwu, A. J., Radjagukguk, C. I., Zai, J. S., Ilham, A., Marunduri, S. R., Cui, N. S., Bate'e, A. L., Hulu, B. S., Laoli, A. M., Mendrofa, M., & Zebua, L. I. S. J. (2025). Setan Scammer: Menghindari Penipuan Online. *JIPMAS: Jurnal Visi Pengabdian Kepada Masyarakat*, *06*(02), 133–145.

Nirwana, D., Nurjannah, E., Renta, C., Marpaung, A., & Wijaya, H. A. (2024). Analisis Kebijakan Keamanan Cyber : Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital. *JIIP (Jurnal Ilmiah Ilmu Pendidikan)*, *7*(7), 7364–7373.

Nofus, N., Safitri, D., & Astuti, D. (2025). Strategi Pemasaran Digital Untuk Meningkatkan Daya Saing UMKM Di Era Transformasi Teknologi. *Jurnal Ekonomi Dan Bisnis Digital*, *12*(01), 1526–1530.

Putri, C. P., Anggraini, W., & Hasibuan, Y. M. (2023). Strategi Pengamanan Cyber : Lingkup Kerjasama dalam Menghadapi Ancaman Cyber. *INSOLOGI: Jurnal Sains Dan Teknologi*, *2*(6), 1124–1130. https://doi.org/10.55123/insologi.v2i6.2847

Sadiani. (2014). *Peran Lembaga Adat Kedamangan Dayak Siang dalam Kawasan Hutan Adat Puruk Kambang di Kabupaten Murung Raya Kalimantan Tengah*. Universitas Brawijaya.

Santoso, J. T. (2023). *Teknologi Keamanan Siber (Cyber Security)*. Yayasan Prima Agus Teknik dengan Universitas STEKOM.

Sumarni, T., dkk. (2024). Menghadapi Ancaman Cyber : Strategi Keamanan Untuk Sistem Pembayaran E-Commerce. *Indonesian Journal of Innovation Science and Knowledge*. 1(4), 15-27.

Tamzil, F., & Deby Aprilia Ningrum, T. (2022). Tingkat Keamanan Teknologi E-Commerce dan Cashless pada Pengguna Android (Studi Kasus Teknologi Informasi Perusahaan dan E-Bussines). *Forum Ilmiah*, *19*(2), 213–224.

Triwahyuni, D., & Wulandari, T. A. (2016). Strategi Keamanan Cyber Amerika Serikat. *Jurnal Ilmu Politik Dan Komunikasi*, *VI*(1).

Utomo, B. C., & Rahman, A. A. (2024). Analisis Kesadaran Keamanan Data Pribadi pada Pengguna E-Wallet DANA. *Jurnal Riset Sains Dan Teknologi*, *8*(2), 155–166.

Wijoyo, A., Abdillah, B., Khalbi, F., Saputra, R. A., & Khoiriyah, W. (2024). Keamanan Cyber Dalam Sistem Informasi Manajemen: Ancaman dan Solusi Terbaru. *Jurnal Ilmiah Wahana Pendidikan*, *10*(23), 1157–1165.

Ychsan, M. A. F. (2021). *Strategi Minimalisasi Risiko Pembelian Berbasis Online Melalui Marketplace Shopee Oleh Mahasiswi Iain Jember*. Universitas Islam Negeri Kiai Achmad Siddiq Jember.

Yurfani, F. T.& Ningrum, T. D. A. (2022). TINGKAT KEAMANAN TEKNOLOGI E-COMMERCE DAN CASHLESS PADA PENGGUNA ANDROID (STUDI KASUS TEKNOLOGI INFORMASI PERUSAHAAN DAN E-BUSSINES). *Forum Ilmiah*. 19(2), 213-224.