JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 599-606
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Analisis Keamanan Siber Pada Akun WhatsApp terhadap Ancaman Pembajakan Melalui OTP dan Social Engineering

Ami Al Rasyid Nasution[1], Abi Raihan Anshari[2], Aldiansah Rambe[3], Inggi Arjul R[4]

[1,2,3,4]Universitas Labuhanbatu, Indonesia

Email: amirasyid2@gmail.com[1], abiraihan200516@gmail.com[2], aldi75633@gmail.com[3], inggilarulr@gmail.com[4]

ABSTRAK

Perkembangan teknologi komunikasi digital meningkatkan penggunaan WhatsApp sebagai media komunikasi utama masyarakat. Namun, tingginya penggunaan aplikasi tersebut juga meningkatkan ancaman keamanan siber, khususnya pembajakan akun melalui penyalahgunaan *One-Time Password* (OTP) dan teknik *social engineering*. Penelitian ini bertujuan menganalisis ancaman keamanan siber pada akun WhatsApp, faktor penyebab pembajakan akun, serta sistem keamanan yang tersedia pada aplikasi tersebut. Metode penelitian yang digunakan adalah penelitian kualitatif dengan pendekatan studi literatur dan studi kasus. Data diperoleh dari jurnal ilmiah, artikel akademik, laporan keamanan digital, dan dokumentasi kasus pembajakan akun WhatsApp. Hasil penelitian menunjukkan bahwa rendahnya kesadaran keamanan digital pengguna menjadi faktor utama keberhasilan pembajakan akun. Teknik phishing, manipulasi psikologis, dan pencurian OTP menjadi metode serangan yang paling sering digunakan. WhatsApp telah menyediakan fitur keamanan seperti *end-to-end encryption* dan *two-step verification*, namun penggunaannya belum optimal. Penelitian ini menyimpulkan bahwa edukasi keamanan siber dan peningkatan kewaspadaan pengguna diperlukan untuk mengurangi risiko pembajakan akun WhatsApp.
Kata Kunci: Keamanan Siber, WhatsApp, OTP, *Social Engineering*

ABSTRACT

The development of digital communication technology has increased the use of WhatsApp as a primary communication medium. However, this high use of the application has also increased cybersecurity threats, particularly account hijacking through misuse of One-Time Passwords (OTPs) and social engineering techniques. This study aims to analyze cybersecurity threats to WhatsApp accounts, the factors causing account hijacking, and the security systems available on the application. The research method used was qualitative research with a literature review and case study approach. Data was obtained from scientific journals, academic articles, digital security reports, and documentation of WhatsApp account hijacking cases. The results indicate that low user digital security awareness is a major factor in account hijacking success. Phishing, psychological manipulation, and OTP theft are the most frequently used attack methods. WhatsApp has provided security features such as end-to-end encryption and two-step verification, but their use has not been optimal. This study concludes that cybersecurity education and increased user awareness are needed to reduce the risk of WhatsApp account hijacking.
Keywords: Cybersecurity, WhatsApp, OTP, Social Engineering

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar terhadap pola interaksi masyarakat, terutama melalui penggunaan

aplikasi pesan instan sebagai media komunikasi digital. Salah satu aplikasi yang memiliki tingkat penggunaan tinggi adalah WhatsApp karena menawarkan layanan komunikasi cepat, berbagi dokumen, panggilan suara, dan video secara mudah. WhatsApp juga menerapkan sistem *end-to-end encryption* yang dirancang untuk menjaga kerahasiaan komunikasi pengguna sehingga hanya pengirim dan penerima yang dapat membaca isi pesan. Namun, tingginya penggunaan WhatsApp menyebabkan aplikasi ini menjadi sasaran berbagai ancaman siber yang memanfaatkan celah teknologi maupun kelemahan pengguna (Fitriyani, 2025).

Kemajuan teknologi digital selain memberikan manfaat juga memunculkan berbagai bentuk kejahatan siber yang semakin kompleks. Ancaman keamanan siber tidak hanya menyerang infrastruktur teknologi, tetapi juga menargetkan identitas digital dan data pribadi pengguna. Dalam konteks aplikasi komunikasi digital, ancaman seperti *phishing*, malware, pencurian identitas, serta penyalahgunaan akun menjadi permasalahan yang sering terjadi. Hal ini menunjukkan bahwa keamanan digital tidak hanya bergantung pada sistem enkripsi yang digunakan, tetapi juga dipengaruhi oleh perilaku pengguna dalam menjaga informasi pribadinya (Nur Islam et al., 2024).

Salah satu bentuk ancaman yang banyak terjadi pada WhatsApp adalah pembajakan akun melalui penyalahgunaan kode *One-Time Password* (OTP) dan teknik *social engineering*. Modus ini dilakukan dengan memanipulasi korban melalui penyamaran identitas, pesan palsu, maupun permintaan kode verifikasi dengan mengatasnamakan pihak tertentu. Ketika korban memberikan kode OTP, pelaku dapat mengambil alih akun dan memanfaatkannya untuk penipuan, penyebaran informasi palsu, maupun pencurian data pribadi. Ancaman ini memperlihatkan bahwa faktor manusia sering kali menjadi titik lemah dalam sistem keamanan digital, meskipun aplikasi telah memiliki lapisan perlindungan teknologi (ZUHRIYANTO & Sri Rahayu Astari, 2025).

Dampak pembajakan akun WhatsApp tidak hanya merugikan korban secara personal, tetapi juga dapat memengaruhi lingkungan sosial dan ekonomi pengguna. Akun yang berhasil diambil alih sering digunakan untuk meminta sejumlah uang kepada kontak korban, menyebarkan tautan berbahaya, hingga melakukan penipuan berkedok pinjaman atau hadiah palsu. Selain kerugian finansial, korban juga berisiko mengalami kebocoran data pribadi serta kehilangan kepercayaan dari lingkungan sosialnya. Oleh karena itu, ancaman pembajakan akun WhatsApp perlu dipandang sebagai masalah keamanan siber yang serius dan membutuhkan upaya mitigasi yang memadai (Integrasi & Lokal, 2025).

Berdasarkan permasalahan tersebut, penelitian mengenai keamanan siber pada akun WhatsApp menjadi penting untuk dilakukan guna memahami pola ancaman pembajakan melalui OTP dan *social engineering* serta mengevaluasi efektivitas sistem keamanan yang tersedia. Penelitian ini bertujuan untuk menganalisis bentuk ancaman, faktor penyebab keberhasilan pembajakan akun, serta upaya pencegahan yang dapat diterapkan pengguna agar keamanan akun tetap terjaga. Dengan adanya

penelitian ini diharapkan dapat meningkatkan kesadaran keamanan digital masyarakat serta memberikan kontribusi terhadap pengembangan strategi perlindungan akun komunikasi digital di era siber modern (Indra Richardo & Amarudin, 2025).

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan studi kasus dan studi literatur (literature review). Pendekatan kualitatif dipilih karena penelitian berfokus pada pemahaman fenomena keamanan siber pada akun WhatsApp, khususnya ancaman pembajakan melalui penyalahgunaan *One-Time Password* (OTP) dan *social engineering*. Studi kasus digunakan untuk mengidentifikasi pola serangan berdasarkan kasus pembajakan akun WhatsApp yang telah terjadi, sedangkan studi literatur digunakan untuk memperoleh teori, konsep, dan hasil penelitian terdahulu yang relevan dengan keamanan siber dan perlindungan akun digital (P et al., 2023).

Penelitian ini tidak melakukan eksperimen laboratorium ataupun pengembangan perangkat lunak, tetapi menitikberatkan pada analisis ancaman, evaluasi sistem keamanan, serta identifikasi faktor yang memengaruhi keberhasilan pembajakan akun digital. Pendekatan kualitatif dinilai sesuai karena kejahatan siber melalui *social engineering* tidak hanya dipengaruhi aspek teknis, tetapi juga perilaku dan tingkat kesadaran keamanan pengguna (Kuswulandari et al., 2023).

Waktu Penelitian

Penelitian dilaksanakan pada 29 Mei 2026. Penelitian tidak dilakukan pada lokasi fisik tertentu karena menggunakan pendekatan studi literatur dan dokumentasi digital. Oleh sebab itu, proses penelitian dilakukan secara daring dengan memanfaatkan sumber data berupa jurnal ilmiah, artikel akademik, laporan keamanan siber, dan dokumentasi kasus pembajakan akun WhatsApp yang tersedia pada basis data ilmiah dan sumber digital terpercaya.

Target/Sasaran Penelitian

Target penelitian ini adalah fenomena keamanan siber yang berkaitan dengan pembajakan akun WhatsApp melalui penyalahgunaan OTP dan teknik *social engineering*. Sasaran penelitian diarahkan pada identifikasi pola ancaman, mekanisme serangan, faktor penyebab keberhasilan pembajakan akun, serta evaluasi sistem keamanan yang tersedia pada WhatsApp. Fokus tersebut dipilih karena pembajakan akun WhatsApp masih menjadi salah satu bentuk kejahatan siber yang sering terjadi dan menimbulkan kerugian bagi pengguna (Firgiawan et al., 2021).

Subjek Penelitian

Subjek penelitian berupa dokumen dan sumber informasi yang berkaitan dengan keamanan siber, WhatsApp, OTP, dan *social engineering*. Sumber data meliputi jurnal ilmiah, prosiding, artikel akademik, laporan keamanan digital, serta dokumentasi kasus pembajakan akun yang dipublikasikan melalui media digital dan sumber ilmiah terpercaya. Pemilihan subjek dilakukan secara purposif berdasarkan relevansi terhadap topik penelitian sehingga data yang diperoleh sesuai dengan kebutuhan analisis (Puguh Ika & Intan, 2021; Rifai et al., 2024).

Subjek Penelitian

Subjek penelitian berupa dokumen dan sumber informasi yang berkaitan dengan keamanan siber, WhatsApp, OTP, dan *social engineering*. Sumber data meliputi jurnal ilmiah, prosiding, artikel akademik, laporan keamanan digital, serta dokumentasi kasus pembajakan akun yang dipublikasikan melalui media digital dan sumber ilmiah terpercaya. Pemilihan subjek dilakukan secara purposif berdasarkan relevansi terhadap topik penelitian sehingga data yang diperoleh sesuai dengan kebutuhan analisis (Prastiwi et al., 2024).

Prosedur Penelitian

Tabel 1. Prosedur Penelitian

Tahap	Aktivitas	Output
Identifikasi Masalah	Menentukan isu pembajakan WhatsApp	Rumusan Masalah
Pengumpulan Data	Studi Literatur dan dokumentasi	Data Penelitian
Analisis Ancaman	Mengidentifikasi OTP dan Social Engineering	Pola Serangan
Evaluasi Keamanan	Menilai Sistem keamanan WhatsApp	Temuan Penelitian
Kesimpulan	Menyusun solusi dan mitigasi	Rekomendasi

Prosedur penelitian dilakukan melalui beberapa tahapan. Tahap pertama adalah identifikasi masalah, yaitu menentukan isu keamanan siber berupa pembajakan akun WhatsApp melalui OTP dan social engineering. Tahap kedua yaitu pengumpulan data melalui studi literatur dan dokumentasi kasus. Tahap ketiga adalah analisis ancaman, yaitu mengkaji bentuk serangan seperti phishing, pencurian OTP, impersonation, dan manipulasi psikologis yang digunakan pelaku. Tahap selanjutnya adalah evaluasi sistem keamanan WhatsApp, termasuk mekanisme end-to-end encryption dan two-step verification. Tahap akhir berupa penyusunan kesimpulan dan rekomendasi pencegahan (Heriadi et al., 2024).

Data dan Instrumen Penelitian

Tabel 2. Data dan Instrumen Penelitian

Jenis Data	Sumber	Instrumen
Data keamanan WhatsApp	Jurnal dan artikel	Cheklist literatur

Data Pembajakan Akun	Dokumentasi kasus	Lembar observasi
Data mitigasi keamanan	Laporan keamanan digital	Format analisis

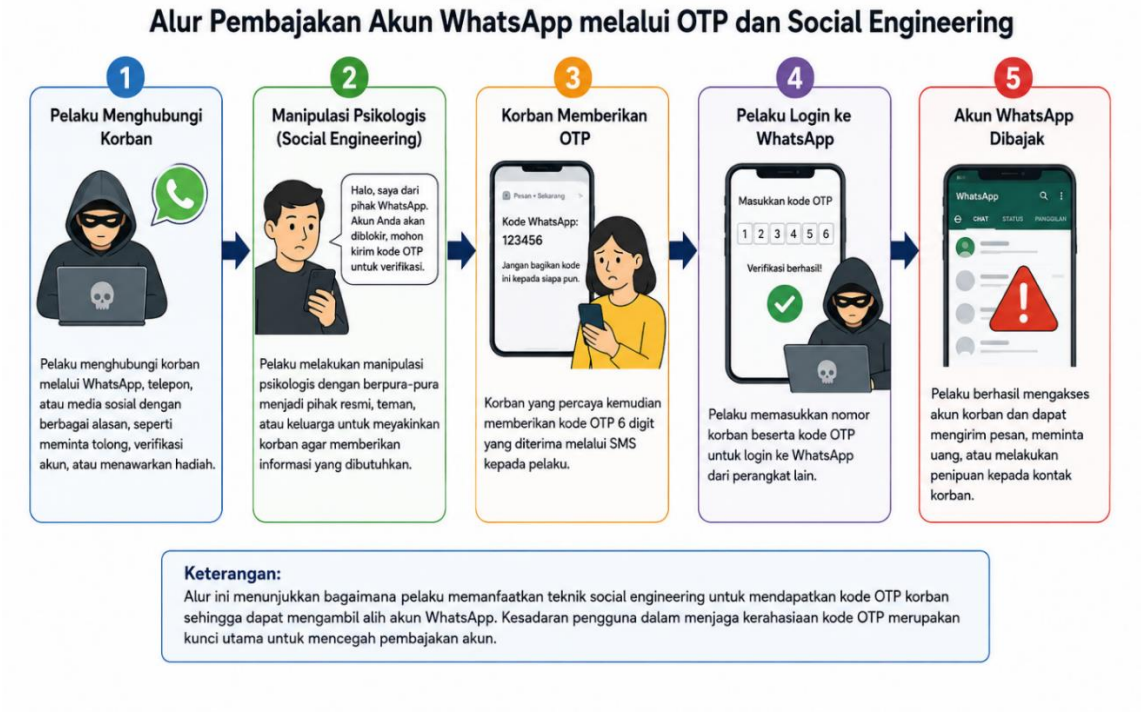
Data penelitian terdiri atas data sekunder yang diperoleh melalui jurnal ilmiah, artikel akademik, dan laporan keamanan digital. Instrumen penelitian menggunakan lembar observasi dokumen dan checklist analisis literatur untuk mencatat informasi mengenai jenis serangan, metode pembajakan, dampak ancaman, serta sistem keamanan yang digunakan pada WhatsApp. Instrumen tersebut digunakan untuk membantu peneliti mengelompokkan data agar analisis dilakukan secara sistematis dan konsisten (Rochmadi et al., 2025).

Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui studi literatur dan dokumentasi. Studi literatur dilakukan dengan menelaah jurnal dan penelitian terdahulu mengenai keamanan siber, perlindungan data, dan pembajakan akun digital. Dokumentasi dilakukan dengan mengumpulkan informasi mengenai kasus pembajakan WhatsApp yang dipublikasikan melalui media digital dan laporan keamanan siber. Teknik ini dipilih karena mampu memberikan gambaran menyeluruh mengenai fenomena pembajakan akun serta mekanisme ancaman yang digunakan pelaku (Teaningrum et al., 2025).

HASIL DAN PEMBAHASAN

Hasil



Gambar 1. Alur Pembajakan Akun WhatsApp melalui OTP dan Social Engineering

Berdasarkan gambar 1. menunjukkan proses pembajakan akun WhatsApp yang dilakukan melalui penyalahgunaan kode OTP dan teknik *social engineering*. Tahap pertama dimulai ketika pelaku menghubungi korban dengan menyamar sebagai pihak tertentu, seperti teman, keluarga, atau layanan resmi. Selanjutnya, pelaku melakukan manipulasi psikologis untuk memperoleh kepercayaan korban dan meminta kode OTP yang dikirimkan melalui SMS. Setelah korban memberikan kode OTP, pelaku dapat masuk ke akun WhatsApp korban dan mengambil alih akun tersebut. Proses ini menunjukkan bahwa keberhasilan pembajakan akun tidak hanya disebabkan oleh kelemahan sistem keamanan, tetapi juga rendahnya kesadaran keamanan digital pengguna.

Berdasarkan analisis keamanan sistem WhatsApp, aplikasi ini sebenarnya telah menyediakan beberapa mekanisme perlindungan, seperti *end-to-end encryption* dan *two-step verification*. Fitur *end-to-end encryption* mampu melindungi isi komunikasi agar tidak dapat dibaca pihak ketiga, sedangkan *two-step verification* memberikan lapisan keamanan tambahan berupa PIN verifikasi. Namun, sistem keamanan tersebut masih dapat dilewati apabila pengguna menjadi korban manipulasi *social engineering*.

Hasil analisis menunjukkan bahwa pencegahan pembajakan akun WhatsApp tidak hanya bergantung pada sistem keamanan aplikasi, tetapi juga pada peningkatan kesadaran keamanan siber pengguna. Edukasi mengenai kerahasiaan OTP, verifikasi identitas pengirim pesan, penggunaan *two-step verification*, serta kewaspadaan terhadap tautan mencurigakan menjadi langkah penting dalam mengurangi risiko pembajakan akun digital.

Pembahasan

Hasil penelitian menunjukkan bahwa faktor manusia (*human factor*) menjadi celah utama dalam kejahatan siber berbasis *social engineering*. Pelaku tidak selalu menyerang sistem teknis secara langsung, melainkan memanfaatkan psikologi korban melalui manipulasi informasi dan rasa panik. Kondisi ini menunjukkan bahwa keamanan digital tidak hanya bergantung pada teknologi, tetapi juga tingkat literasi keamanan pengguna.

Pembajakan akun WhatsApp melalui OTP menunjukkan bahwa autentikasi berbasis kode verifikasi masih memiliki kelemahan apabila pengguna tidak memahami prosedur keamanan digital. Dalam banyak kasus, korban secara sadar memberikan OTP kepada pelaku karena percaya terhadap identitas palsu yang digunakan. Hal ini membuktikan bahwa serangan *social engineering* lebih menargetkan kelemahan manusia dibandingkan kelemahan sistem.

Fitur keamanan WhatsApp seperti *end-to-end encryption* dan *two-step verification* sebenarnya cukup efektif dalam melindungi akun pengguna. Namun, efektivitas fitur tersebut bergantung pada penerapan dan kesadaran pengguna. Banyak pengguna belum mengaktifkan *two-step verification*, sehingga akun menjadi lebih mudah diambil alih ketika OTP berhasil diperoleh pelaku.

Penelitian ini juga menunjukkan bahwa perkembangan teknologi komunikasi

digital memberikan dampak positif sekaligus meningkatkan risiko ancaman siber. Tingginya penggunaan WhatsApp dalam aktivitas sehari-hari menjadikan aplikasi ini sebagai target utama pelaku kejahatan siber. Oleh karena itu, diperlukan peningkatan edukasi keamanan siber secara berkelanjutan agar pengguna lebih memahami risiko phishing, pencurian OTP, dan manipulasi digital.

Berdasarkan hasil penelitian, strategi pencegahan yang dapat dilakukan meliputi peningkatan literasi keamanan digital, aktivasi *two-step verification*, tidak membagikan kode OTP kepada pihak lain, serta meningkatkan kewaspadaan terhadap tautan atau file mencurigakan. Dengan kombinasi antara sistem keamanan aplikasi dan kesadaran pengguna, risiko pembajakan akun WhatsApp dapat diminimalkan.

KESIMPULAN

Berdasarkan hasil penelitian mengenai "Analisis Keamanan Siber pada Akun WhatsApp terhadap Ancaman Pembajakan melalui OTP dan Social Engineering", dapat disimpulkan bahwa pembajakan akun WhatsApp masih menjadi salah satu ancaman keamanan siber yang sering terjadi. Serangan dilakukan melalui penyalahgunaan kode OTP (*One-Time Password*) dan teknik *social engineering* yang memanfaatkan kelemahan pengguna dalam menjaga kerahasiaan informasi autentikasi akun.

Hasil penelitian menunjukkan bahwa faktor manusia menjadi penyebab utama keberhasilan pembajakan akun WhatsApp. Rendahnya literasi keamanan digital, kurangnya kewaspadaan terhadap pesan mencurigakan, serta kebiasaan memberikan kode OTP kepada pihak lain menyebabkan akun pengguna mudah diambil alih oleh pelaku kejahatan siber. Selain itu, teknik phishing, impersonation, dan manipulasi psikologis menjadi metode yang paling sering digunakan dalam proses pembajakan akun digital.

WhatsApp sebenarnya telah menyediakan beberapa fitur keamanan seperti *end-to-end encryption* dan *two-step verification* untuk melindungi akun pengguna. Namun, efektivitas sistem keamanan tersebut sangat bergantung pada tingkat kesadaran dan pemahaman pengguna terhadap keamanan digital. Apabila pengguna tidak memahami pentingnya menjaga kerahasiaan OTP dan tidak mengaktifkan fitur keamanan tambahan, maka risiko pembajakan akun akan semakin tinggi.

Penelitian ini juga menunjukkan bahwa upaya pencegahan pembajakan akun WhatsApp perlu dilakukan melalui peningkatan edukasi keamanan siber kepada masyarakat. Pengguna disarankan untuk tidak membagikan kode OTP kepada siapa pun, mengaktifkan fitur *two-step verification*, serta lebih waspada terhadap tautan, file, atau pesan mencurigakan yang berpotensi mengandung unsur phishing maupun manipulasi digital. Dengan kombinasi antara sistem keamanan aplikasi dan kesadaran pengguna, ancaman pembajakan akun WhatsApp dapat diminimalkan.

DAFTAR PUSTAKA

Firgiawan, R., Ananda, G., & Sulistiyani, E. (2021). *ANALISIS KEAMANAN TERHADAP KOMBINASI XSS DAN SOCIAL*. 367–374.

Fitriyani, R. (2025). Analisis Keamanan WhatsApp di Berbagai Platform: Studi Kasus Serangan dan Perlindungan Data Pengguna. *Ikhraith-Informatika*, *9*(2), 116–122.

Heriadi, S. A., Azizah, F. A., & Septyadi, F. E. (2024). Penerapan Kriptografi Dalam Menanggulangi Ancaman Cyber " Undangan Non Aplikasi ." *Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB)*, 555–560.

Indra Richardo, K., & Amarudin, A. (2025). Analisis Serangan Social Engineering melalui Pretexting, Impersonating, dan Phishing pada Pemain Game Mobile Online. *Jurnal Pendidikan Dan Teknologi Indonesia*, *5*(7), 1993–2003. https://doi.org/10.52436/1.jpti.892

Integrasi, D., & Lokal, B. (2025). *Melek IT*. *11*(1), 101–112.

Kuswulandari, R., Wirid, A., Jowanka, I., Nabila, T., Riyanto, P., & Listiani, T. (2023). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp. *Prosiding Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB)*, 72–78.

Nur Islam, P., Dwi Ahwadti, R., & Rizky Adjie Prakoso, M. (2024). *Analisis Dampak Kesadaran Keamanan Informasi User Whatsapp terhadap penyebaran Phising Malware "Undangan.APK."* 18–2024.

P, M. G. B., Hafizh, M., Mustofa, A., Saputra, R., & Wardani, S. N. (2023). *A nalis R esiko K eamanan P ada E- commerce S hopee Terhadap K enyamaan K onsumen M enggunakan Metode Kualitatif*. 79–83.

Prastiwi, Y., Yuan Varel, E., & Nainggolan, H. (2024). Analisis Keamanan Data Pribadi Dalam Aplikasi Mobile "Dana." *In Prosiding Seminar Nasional Teknologi Informasi Dan Bisnis*, 584–588.

Puguh Ika, L., & Intan, S. (2021). 1257-Article Text-1677-1-10-20210903. *Sistem Keamanan Simrs Di Rumah Sakit*, 234–240.

Rifai, M. H. ., Pramudya, D. A., & Narfandi, R. . (2024). Analisis peran teknologi kecerdasan buatan dalam mengoptimalkan proses deteksi terhadap serangan siber. *Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB)*, 495–502.

Rochmadi, T., Ardiyaningrum, M., Mulyandari, R., & Miju, S. (2025). *Pengukuran Kesadaran Keamanan Informasi UMKM terhadap Phising pada Aplikasi Whatsapp*. *11*, 184–190.

Teaningrum, R. Y., Pebrianggara, A., & Oetarjo, M. (2025). The Influence of Usability, E-Satisfaction and E-Security on E-Loyalty of WhatsApp Mobile Instant Messaging Users. *Jurnal Ilmiah Manajemen Kesatuan*, *13*(1), 519–530. https://doi.org/10.37641/jimkes.v13i1.3021

ZUHRIYANTO, I., & Sri Rahayu Astari. (2025). Penerapan Zero Trust Architecture untuk Mitigasi Ancaman Pembajakan Akun WhatsApp. *JITU : Journal Informatic Technology And Communication*, *9*(1), 50–58. https://doi.org/10.36596/jitu.v9i1.1815