P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v9i2

Analisis Keamanan WhatsApp di Berbagai Platform: Studi Kasus Serangan dan Perlindungan Data Pengguna

Rofi Fitriyani,

Informatika, Universitas Majalengka, Majalengka

E-mail: fitriyanirofi@gmail.com

ABSTRAK

Salah satu aplikasi pesan instan sangat populer di dunia yaitu WhatsApp, yang tersedia di berbagai platform seperti Web, Android, dan iOS, semakin rentan terhadap ancaman keamanan seperti phishing, malware, eksploitasi enkripsi, dan kebocoran data pengguna. Tujuan dari penelitian ini adalah untuk memeriksa keamanan WhatsApp di berbagai platform dengan mengidentifikasi jenis serangan yang paling umum dan mengevaluasi metode yang telah digunakan untuk melindungi data. Penelitian ini menggunakan studi literatur dan analisis forensik digital. Studi menunjukkan bahwa peretas dapat menggunakan celah keamanan WhatsApp terutama melalui rekayasa sosial dan eksploitasi pihak ketiga meskipun WhatsApp menggunakan enkripsi end-to-end dan fitur keamanan lainnya. Oleh karena itu, untuk meminimalkan risiko keamanan, kesadaran pengguna harus ditingkatkan dan mekanisme perlindungan data harus diperkuat.

Kata kunci : ***Keamanan WhatsApp, Enkripsi End-To-End, Phishing, Malware***

ABSTRACT

One of the most popular instant messaging applications in the world, WhatsApp, which is available on various platforms such as Web, Android, and iOS, is increasingly vulnerable to security threats such as phishing, malware, encryption exploitation, and user data leaks. The purpose of this research is to examine the security of WhatsApp across various platforms by identifying the most common types of attacks and evaluating the methods that have been used to protect data. This research utilizes literature studies and digital forensic analysis. Studies show that hackers can exploit WhatsApp's security vulnerabilities primarily through social engineering and third-party exploitation, even though WhatsApp employs end-to-end encryption and other security features. Therefore, to minimize security risks, user awareness must be enhanced, and data protection mechanisms must be strengthened.

Keyword : ***The security of WhatsApp, End-to-End Encryption, Phishing, Malware***

1. PENDAHULUAN

Dunia digital sudah memberikankemudahan melalui teknologi, khusunya dengan keberadaan smartphone yang berperan besar. Android ialah sistem operasi yang dominan di Indonesia, tetapi penggunaannya yang luas turut memberikan peningkatan terhadap potensi kerentanan keamanan, khususnya dikarenakan banyak pengguna yang kurang memahami keamanan data

(Prayudi, 2025). Era digital sudah menghadirkan perubahan signifikan dalam cara komunikasi serta interaksi sosial. Tetapi, perkembangan tersebut turut menghadirkan tantangan baru dalam wujud ancaman keamanan siber, misalnya phishing (Febrika Ardy et al., 2024). Serangan phising melalui WhatsApp di Indonesia menjadi semakin marak dan canggih. Modus operandi yang digunakan para penjahat siber melibatkan pengiriman pesan teks yang mengandung tautan mencurigakan yang mengarahkan korban ke situs web palsu yang dibuat agar dapat mencuri informasi pribadi dan finansial (Isadora et al., n.d.). Kejahatan phising merupakan kejahatan Cyber Crime yang terjadi di dunia digital. Perlindungan pengguna media sosial terhadap kejahatan phising diatur dalam Undang-Undang ITE dan Undang-Undang perlindungan data pribadi (Reyhan & Gultom, n.d.).

Perkembangan pesat dalam pemanfaatan teknologi informasi dalam kebutuhan informasi di lingkungan masyarakat pedesaan sangat penting (Panji Novantara & Tito Sugiharto, 2025). Kesadaran keamanan informasi di kalangan pengguna WhatsApp berperan besar dalam mencegah penyebaran phishing malware dalam bentuk undangan.apk di Indonesia. WhatsApp, selaku platform pesan instan yang populer, kerap kali menjadi sasaran serangan siber (Nur Islam et al., n.d.).

Di Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mengatur mengenai perundungan siber; namun, implementasinya menghadapi berbagai tantangan. Hambatan utama dalam penegakan hukum mencakup kesulitan dalam mengidentifikasi pelaku yang menggunakan identitas anonim, kurangnya koordinasi antara platform media sosial dan lembaga penegak hukum, serta rendahnya kesadaran masyarakat mengenai mekanisme pelaporan (Marjun et al., 2025). Pencurian data privasi melalui media sosial WhatsApp dalam bentuk URL atau tautan, serta file undangan dalam format PDF, menjadi pendorong penelitian ini. Oleh karena itu, diperlukan penanganan lebih lanjut melalui manajemen keamanan agar penipuan ini dapat diselesaikan dengan baik. Penipuan ini sangat umum terjadi, sehingga untuk melindungi pengguna dari serangan phishing, penting untuk memahami modus phishing di WhatsApp dan mengembangkan metode keamanan yang lebih baik. Ancaman phishing merupakan salah satu jenis penipuan online yang sering terjadi melalui WhatsApp Messenger (Manajemen et al., 2024). Penipuan tilang online melalui WhatsApp merupakan kejahatan yang meresahkan dan merugikan masyarakat. Penipuan tilang online yang marak terjadi akhir - akhir ini menjadi ancaman yang semakin serius di era digital pada saat ini dan menimbulkan kerugian bagi korban salah satunya adalah kerugian finansial karena terjerat penipuan tilang online. Oleh karena itu, upaya pencegahan dan mitigasi menjadi sangat penting untuk melindungi masyarakat dari modus penipuan ini. Pentingnya meningkatkan edukasi dan literasi masyarakat tentang penipuan online, meningkatkan patroli cyber dan penegakan hukum terhadap pelaku penipuan online dapat menjadi solusi untuk mencegah terjadinya penipuan tilang online via WhatsApp (Hafiz Rahmadani et al., n.d.).

Maka perlu adanya penerapan enkripsi end-to-end pada aplikasi chatting yang akan membuktikan efektivitasnya dalam melindungi keamanan data pengguna dengan tingkat yang tinggi. Perihal tersbut terbukti dari kemampuan enkripsi end-toend dalam melindungi pesan-pesan yang dikirimkan, sehingga hanya pengirim serta penerima yang dapat membaca isi pesan tersebut, melindungi kerahasiaan informasi yang terdapat di dalamnya. Di sisi lain, enkripsi endto-end juga

P-ISSN :2580-4316
E-ISSN :2654-8054
10.37817/ikraith-informatika.v9i2

melindungi secara kuat beragam serangan misalnya peretasan maupnn penyadapan data di tengah perjalanan (Juniarmi, 2024).

WhatsApp, sebagai sebuah aplikasi pesan instan paling populer, menghadapi berbagai ancaman keamanan seperti phishing, malware, dan kebocoran data. Penelitian ini menganalisis keamanan WhatsApp di berbagai platform dengan mengidentifikasi jenis serangan umum serta mengevaluasi metode perlindungan seperti enkripsi end-to-end. Melalui studi literatur dan analisis forensik digital. Meskipun WhatsApp telah menerapkan berbagai fitur keamanan, serangan phishing, malware, dan kebocoran data masih dapat terjadi. Oleh karena itu, kesadaran pengguna perlu ditingkatkan, dan perlindungan data harus diperkuat untuk mengurangi risiko keamanan.

Adapun metode perlindungan yang dibahas dalam hasil serta pembahasan mencakup enkripsi end-to-end, verifikasi dua langkah, dan pembaruan keamanan berkala. Ketiga metode ini merupakan upaya WhatsApp untuk meningkatkan keamanan data pengguna serta melindungi mereka dari berbagai ancaman siber.

Hasil penelitian ini membawa harapan agar mampu berperan sebagai panduan bagi para profesional keamanan dalam mengelola risiko siber secara lebih efektif.

2. LANDASAN TEORI

Keberadaan layanan pesan instan yang merajalela di perangkat mobile dan penggunaan enkripsi ujung-ke-ujung (end-to-end encryption/E2EE) dalam melindungi privasi pengguna telah menjadi perhatian bagi beberapa pemerintah. Layanan pesan WhatsApp telah muncul sebagai aplikasi pesan paling populer di perangkat mobile saat ini. WhatsApp menggunakan enkripsi ujung-ke-ujung yang membuat upaya pemerintah dan dinas rahasia untuk memerangi kejahatan terorganisir, teroris, dan pelaku pornografi anak menjadi mustahil secara teknis. Pemerintah menginginkan "pintu belakang" (backdoor) ke dalam aplikasi semacam itu, untuk digunakan dalam mengakses pesan, dan menekankan bahwa mereka hanya akan menggunakan "pintu belakang" jika ada ancaman kredibel terhadap keamanan nasional (Endeley, 2018).

Serangan keamanan terus muncul setiap hari karena pertumbuhan pesat dalam jumlah perangkat pintar dan aplikasi seluler. Aplikasi semacam ini hanya membutuhkan dua izin yang mencakup "Akses Notifikasi" dan "Internet". Izin ini digunakan untuk mengekstrak dan mengirim pesan pengguna dari aplikasi lain ke email penyerang melalui Internet (Abualola et al., 2016).

Phising merupakan sebuah ancaman yang berbahaya serta yang sangat umum terjadi. Phishing melakukan eksploitasi terhadao setiap orang yang dituju dengan trik menipu agar dapat mencuri data pribadi (Kurnia Sujiwana et al., 2024).

3. METODOLOGI

Penelitian ini memakai pendekatan kualitatif dengan metode studi literatur serta analisis forensik digital agar dapat mengevaluasi tingkat keamanan WhatsApp di berbagai platform, termasuk Web, Android, dan iOS. Metode ini dipilih untuk memperoleh pemahaman yang komprehensif mengenai ancaman keamanan yang dihadapi oleh pengguna WhatsApp serta efektivitas sistem perlindungan yang telah diterapkan.

Studi Literatur

Studi literatur dilakukan dengan meninjau berbagai sumber misalnya laporan keamanan siber, dokumentasi teknis, jurnal ilmiah, serta artikel yang membahas ancaman keamanan terhadap WhatsApp. Literatur yang dikumpulkan dianalisis untuk mengidentifikasi pola

serangan yang umum terjadi dan metode perlindungan yang telah diterapkan oleh WhatsApp maupun pihak ketiga.

Analisis Forensik Digital
Analisis forensik digital dilakukan dengan menguji berbagai skenario serangan pada WhatsApp, termasuk phishing, malware, serta eksploitasi enkripsi. Data dikumpulkan dari berbagai perangkat dan platform (Web, Android, dan iOS) untuk mengidentifikasi potensi celah keamanan dan dampaknya terhadap pengguna.

Hasil dari kedua metode ini dianalisis untuk memberikan rekomendasi peningkatan keamanan serta meningkatkan kesadaran pengguna dalam melindungi data pribadi mereka.

4. HASIL DAN PEMBAHASAN

Studi Literatur
Studi literatur yang dilakukan berhasil mengidentifikasi beberapa ancaman keamanan utama yang dihadapi oleh pengguna WhatsApp, serta metode perlindungan yang telah diterapkan. Berikut adalah temuan utama

1. Ancaman Keamanan yang Teridentifikasi
   - Phishing: Serangan phishing sering terjadi melalui pesan yang menipu pengguna untuk membagikan kode verifikasi atau informasi sensitif lainnya.
   - Malware: Aplikasi modifikasi WhatsApp (seperti GB WhatsApp) menjadi vektor utama penyebaran malware.
   - Kebocoran Data: Eksploitasi metadata dan celah keamanan di server WhatsApp telah menyebabkan kebocoran data pengguna.

2. Metode Perlindungan yang Diterapkan
   - Enkripsi End-to-End: WhatsApp menggunakan protokol Signal untuk memastikan pesan hanya dapat dibaca oleh pengirim dan penerima.
   - Verifikasi Dua Langkah: Fitur ini membantu mencegah akses tidak sah ke akun pengguna.
   - Pembaruan Keamanan Berkala: WhatsApp secara rutin merilis pembaruan untuk menutupi celah keamanan.

Tabel 1. Ancaman dan Metode Perlindungan

Ancaman	*Metode Perlindungan*	*Efektivitas*
Phishing	Verifikasi dua langkah, edukasi pengguna	Tinggi (jika pengguna waspada)
Malware	Pembaruan keamanan, blokir aplikasi modifikasi	Sedang (tergantung kesadaran pengguna)
Kebocoran Data	Enkripsi end-to-end, perlindungan metadata	Rendah (metadata masih rentan)

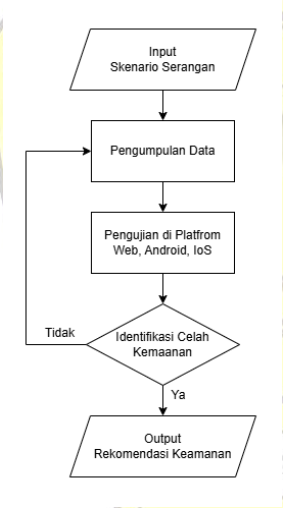
Analisis Forensik Digital
Analisis forensik digital dilakukan dengan
menguji tiga skenario serangan pada WhatsApp di platform Web, Android, dan iOS. Berikut adalah temuan utama

1. Phishing
   - Metode: Pengiriman tautan berbahaya melalui pesan WhatsApp.
   - Hasil: Pengguna di platform Web lebih rentan karena kurangnya fitur deteksi otomatis dibandingkan aplikasi mobile.
   - Rekomendasi: Meningkatkan fitur deteksi phishing di WhatsApp Web.

2. Penyebaran Malware

- Metode: Pengiriman file APK modifikasi melalui WhatsApp.
- Hasil: Pengguna Android lebih rentan karena kemudahan menginstal aplikasi dari sumber tidak resmi.
- Rekomendasi: Blokir pengiriman file APK melalui WhatsApp.

3. Eksploitasi Enkripsi
   - Metode: Mencoba memecahkan enkripsi end-to-end dengan mengeksploitasi metadata.
   - Hasil: Metadata (seperti waktu pengiriman dan penerima) masih rentan terhadap eksploitasi.
   - Rekomendasi: Meningkatkan perlindungan metadata dengan enkripsi tambahan.



Gambar1.Diagram alir Analisis Digital Forensik

Berdasarkan hasil studi literatur dan analisis forensik digital, dapat disimpulkan bahwa WhatsApp telah menerapkan berbagai mekanisme keamanan yang efektif, seperti enkripsi end-to-end maupun verifikasi dua langkah. Namun, masih terdapat celah keamanan yang perlu diperhatikan, terutama pada platform Web dan penggunaan aplikasi modifikasi.

Tantangan Utama

1. Kesadaran Pengguna: Banyak pengguna tidak menyadari risiko penggunaan aplikasi modifikasi atau membagikan kode verifikasi.
2. Kerentanan Metadata: Meskipun pesan terenkripsi, metadata masih dapat dieksploitasi oleh pihak ketiga.
3. Perbedaan Platform: WhatsApp Web memiliki tingkat keamanan yang lebih rendah dibandingkan aplikasi mobile.

Tabel 2. Perbandingan Tingkat Perlindungan di Berbagai Platfrom

Platform	*Tingkat Keamanan*	*Ancaman Utama*	*Rekomendasi*
Web	Rendah	Phishing, Kebocoran Data	Deteksi phishing, enkripsi metadata
Android	Sedang	Malware, Aplikasi Modifikasi	Blokir file APK, edukasi pengguna
iOS	Tinggi	Phishing	Verifikasi dua langkah, pembaruan rutin

Rekomendasi

1. Edukasi Pengguna: WhatsApp perlu meningkatkan kampanye kesadaran keamanan bagi pengguna.
2. Perlindungan Metadata: Menerapkan enkripsi tambahan untuk melindungi metadata.
3. Peningkatan Fitur Keamanan di WhatsApp Web: Menambahkan fitur deteksi phishing dan blokir file berbahaya.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa meskipun WhatsApp telah menerapkan berbagai fitur keamanan, masih terdapat

celah yang perlu diperbaiki, terutama dalam hal perlindungan metadata dan kesadaran pengguna. Dengan mengimplementasikan rekomendasi yang diusulkan, tingkat keamanan WhatsApp dapat ditingkatkan secara signifikan.

6. UCAPAN TERIMA KASIH

Dengan diiringi rasa syukur, penulis menghaturkan ucapan terima kasih kepada semua pihak yang telah mencurahkan dukungan dalam penyusunan paper ini.

Ucapan terima kasih turut disampaikan kepada keluarga yang senantiasa memberikan semangat serta motivasi selama proses penulisan. Tak lupa, apresiasi diberikan kepada berbagai sumber referensi yang telah menjadi dasar dalam penyusunan paper ini.

Semoga penelitian ini mampu bermanfaat bagi pengembangan keamanan digital, terutama dalam memahami tantangan serta solusi perlindungan data pengguna WhatsApp di berbagai platform.

DAFTAR PUSTAKA

Abualola, H., Alhawai, H., Kadadha, M., Otrok, H., & Mourad, A. (2016). An Android-based Trojan Spyware to Study the NotificationListener Service Vulnerability. *Procedia Computer Science*, *83*, 465–471. https://doi.org/10.1016/j.procs.2016.04.210

Endeley, R. E. (2018). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security*, *09*(01), 95–99. https://doi.org/10.4236/jis.2018.91008

Febrika Ardy, L. A., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial. *Journal of Internet and Software Engineering*, *1*(4), 11. https://doi.org/10.47134/pjise.v1i4.2753

Hafiz Rahmadani, F., Cahya Sutany, H., Ragil Aditya, M., Adita Fajar, M., & Ulan Dari, Y. (n.d.). Cybercrime: Analisis Dan Mitigasi Resiko Penipuan Tilang Online Melalui Aplikasi WhatsApp (WA). *23 JSIG |*, *3*(1), 2025. https://ojs.unigal.ac.id/index.php/jsig/index

Isadora, K., Putri Aqila, N., Gustina, H., & Nabila, A. (n.d.). *Analisis Modus Phising terhadap Whatsapp*. https://akuntansi.pnp.ac.id/jabei

Juniarmi, I. (2024). Analisis Keamanan Data pada Aplikasi Chatting Menggunakan Enkripsi End-to-End. *Technologia Journal: Jurnal Informatika*, *1*(2), 3046–9163. https://doi.org/10.62872/ppr42775

Kurnia Sujiwana, R., Fahmi, A., Ridho, A., Aryanti, D. C., & Rakhmawati, N. A. (2024). Analisis Bibliometrik Mengenai Serangan Phishing dan Whatsapp menggunakan Vosviewer. In *Jurnal Esensi Infokom* (Vol. 8, Issue 1).

Manajemen, K., Waspadai, S., Kejahatan, M., Dengan, P., Linkenter, M. B., Trianurahmah, A., Fauzi, A., Tyas, E. N., Suryanto, M. A., Rizky, M., & Wibisono, P. (2024). *Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi* (Vol. 1, Issue 10). https://inovanpublisher.org/orbit

Marjun, Saroji, & Farhan, F. (2025). Cyberbullying and Legal Protection for Victims in the Digital Era: A Case Study on Social Media Platforms. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(1), 955–973. https://doi.org/10.51903/hakim.v3i1.2290

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

Panji Novantara, & Tito Sugiharto. (2025). Pengenalan Keamanan Informasi Digital dalam Peningkatan Resiliensi Cyber di Masyarakat Desa. *ORAHUA : Jurnal Pengabdian Kepada Masyarakat*, *2*(02), 84–89. https://doi.org/10.70404/orahua.v2i02.119

Prayudi, Y. (2025). *Penggunaan Metode Reverse Engineering untuk Analisis*

Aplikasi .apk dalam Meningkatkan Keamanan Perangkat Android.

Reyhan, E., & Gultom, P. (n.d.). *Lex Laguens: Jurnal Kajian Hukum dan Keadilan PERLINDUNGAN HUKUM TERHADAP PENGGUNA SOSIAL MEDIA TERKAIT CYBER CRIME PHISING BERDASARKAN UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK*. *3*, 111–124. https://jurnal.dokterlaw.com/index.php/lexlaguens