Analisis Dampak Kesadaran Keamanan Informasi User Whatsapp terhadap penyebaran Phising Malware "Undangan.APK"

Pria Nur Islam[1], Ringgyanita Dwi Ahwadti[2], Mochammad Rizky Adjie Prakoso[3]

[1]*Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta*
[1]*220103184@mhs.udb.ac.id*

[2]*Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta*
[2]*220103187@mhs.udb.ac.id*

[3]*Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta*
[3]*220103198@mhs.udb.ac.*

Abstrak— Kesadaran keamanan informasi di kalangan pengguna WhatsApp memainkan peran penting dalam mencegah penyebaran phishing malware berbentuk undangan.apk di Indonesia. WhatsApp, sebagai platform pesan instan yang populer, sering menjadi target serangan siber. Penelitian ini bertujuan untuk memahami tingkat kesadaran pengguna tentang ancaman keamanan informasi dan perilaku mereka dalam menghadapi pesan phishing dan malware. Data dikumpulkan melalui survei kuesioner yang melibatkan 103 responden pada Juni 2024. Hasil menunjukkan bahwa mayoritas pengguna WhatsApp merasa cukup aman menggunakan aplikasi tersebut, meskipun pemahaman mendalam tentang enkripsi dan kebijakan privasi masih terbatas. Insiden keamanan yang pernah dialami oleh 15% responden mengindikasikan perlunya peningkatan fitur keamanan dan respons cepat terhadap insiden. Upaya edukasi dan peningkatan fitur keamanan tambahan, seperti otentikasi dua faktor dan notifikasi aktivitas mencurigakan, sangat diperlukan untuk mengurangi risiko serangan siber dan menjaga informasi pribadi pengguna tetap aman.

Kata kunci : Keamanan Informasi, Serangan Siber, Kejahatan Siber, Phising, Malware, Whatsapp.

Abstract— Awareness of information security among WhatsApp users plays a crucial role in preventing the spread of phishing malware in the form of invitation.apk in Indonesia. WhatsApp, as a popular instant messaging platform, often becomes a target for cyber attacks. This research aims to understand the level of user awareness about information security threats and their behavior when dealing with phishing and malware messages. Data was collected through a questionnaire survey involving 103 respondents in June 2024. The results show that the majority of WhatsApp users feel fairly secure using the application, although their deep understanding of encryption and privacy policies is still limited. Security incidents experienced by 15% of respondents indicate the need for enhanced security features and a quick response to incidents. Efforts in education and the addition of security features, such as two-factor authentication and suspicious activity notifications, are highly needed to reduce the risk of cyber attacks and keep users' personal information safe.

Keywords: Information Security, Cyber Attacks, Cybercrime, Phishing, Malware, WhatsApp.

I. PENDAHULUAN

Dalam era digital yang semakin berkembang, media sosial telah menjadi bagian integral dari kehidupan sehari-hari bagi banyak orang. Dengan kemampuannya untuk menghubungkan individu dari seluruh penjuru dunia, menyebarkan informasi secara cepat, dan menyediakan platform untuk berbagi pemikiran serta pengalaman, media sosial telah mengubah cara kita berkomunikasi dan berinteraksi dengan lingkungan sekitar kita. Namun, kemajuan teknologi dan konektivitas ini juga menghadirkan risiko dan tantangan baru, terutama dalam hal keamanan informasi pengguna. Di balik manfaatnya yang besar, media sosial juga menjadi target utama bagi peretas, penipu, dan pelaku kejahatan siber lainnya.[1].

WhatsApp Messenger, sebagai salah satu platform utama dalam media sosial, memberikan kemudahan bagi pelaku penipuan online untuk melakukan kejahatannya. WhatsApp adalah layanan pesan instan lintas platform yang dapat diakses secara gratis untuk ponsel pintar[2]. Badan Siber dan Sandi Negara (BSSN) melaporkan adanya serangan terhadap perangkat Android pengguna melalui pesan phishing yang dikirim melalui WhatsApp, sebuah platform pesan instan yang sangat populer di Indonesia. Pada tahun 2023, Indonesia menempati peringkat ketiga di dunia dalam jumlah pengguna WhatsApp, mencapai 112 juta pengguna[3].

Cybercrime adalah bentuk kejahatan yang menggunakan internet sebagai medium untuk melakukan berbagai tindakan kriminal. Ini

mencakup kejahatan digital dan pelanggaran yang melibatkan jaringan telekomunikasi.[4]. Phishing dan malware adalah dua bentuk utama dari kejahatan di dunia digital. Phishing adalah strategi manipulatif yang mengelabui pengguna untuk mengungkapkan informasi pribadi mereka, yang kemudian dapat digunakan untuk mengakses data atau mencuri identitas. Sementara itu, malware merupakan perangkat lunak berbahaya yang diciptakan untuk tujuan khusus, seperti pencurian data atau merusak sistem, yang sering digunakan untuk menguji tingkat keamanan suatu sistem[5].

Data dapat diretas melalui aplikasiWhatsApp yang terhubung ke internet. Ada berbagai modus operandi yang digunakan, salah satunya melalui undangan atau foto berformat APK yang dikirim melalui WhatsApp. Ketika pengguna tidak sengaja mengklik undangan tersebut, data pribadi dapat dikirimkan kepada pengirim atau peretas yang mengirim undangan tersebut[6]. Korban diminta untuk mengklik dan menginstal aplikasi tersebut. Setelah itu, korban harus menyetujui izin akses terhadap beberapa aplikasi, sehingga data pribadi yang bersifat rahasia di ponsel dapat diambil oleh pelaku. Informasi yang dicuri meliputi berbagai data pribadi dan informasi yang diterima melalui SMS, termasuk data perbankan yang sensitif seperti One Time Password (OTP) dan data lainnya[7].

Penelitian ini bertujuan untuk menganalisis dampak kesadaran keamanan informasi pengguna WhatsApp terhadap penyebaran phishing malware “Undangan.APK” di Indonesia. Dengan memahami tingkat kesadaran dan perilaku pengguna, penelitian ini berharap dapat memberikan rekomendasi yang efektif untuk meningkatkan keamanan informasi dan mengurangi risiko serangan siber. Rumusan masalah yang diangkat meliputi: bagaimana tingkat kesadaran pengguna WhatsApp di Indonesia terhadap ancaman phishing malware seperti undangan.apk, perilaku pengguna WhatsApp dalam menghadapi pesan phishing dan malware, serta dampak penyebaran phishing malware “Undangan.APK” terhadap keamanan informasi pengguna di Indonesia. Penelitian ini dibatasi pada pengguna WhatsApp di Indonesia pada tahun 2023, khususnya kasus penyebaran phishing malware undangan.apk melalui platform tersebut, dan akan menggunakan data dari survei melalui penyebaran kuesioner mengenai tingkat kesadaran keamanan informasi dan pengalaman pengguna terkait serangan malware “Undangan APK”.

II. METODOLOGI PENELITIAN

1. Metode Deskriptif

Metode deskriptif adalah pendekatan yang digunakan untuk menggambarkan gejala atau peristiwa yang sedang diamati selama penelitian [8]. Penelitian deskriptif bertujuan untuk membuat deskripsi yang sistematis, faktual, dan akurat mengenai karakteristik dan kondisi populasi di suatu wilayah tertentu[9].Metode deskriptif digunakan untuk menggambarkan tingkat kesadaran keamanan informasi di kalangan pengguna WhatsApp serta mekanisme penyebaran phishing malware dalam bentuk “Undangan.APK".

2. Metode Kuantitatif

Metode kuantitatif adalah pendekatan penelitian yang didasarkan pada filsafat positivisme, digunakan untuk menginvestigasi populasi atau sampel tertentu dengan pengambilan sampel acak, pengumpulan data menggunakan instrumen penelitian, dan analisis menggunakan pendekatan kuantitatif atau statistik. Tujuan utama metode ini adalah menguji hipotesis yang telah dirumuskan, mengembangkan model matematis, memahami hubungan antar variabel dalam populasi, serta membantu dalam desain penelitian yang tepat[10]. Metode kuantitatif dalam penelitian ini bertujuan untuk mengukur dan menganalisis hubungan antara kesadaran keamanan informasi pengguna WhatsApp dan penyebaran phishing malware dalam bentuk “Undangan.APK”.

3. Metode Pengumpulan Data

Metode penelitian yang digunakan adalah survei, dimana tujuannya adalah untuk mendapatkan

informasi yang representatif dari sejumlah responden yang mewakili populasi tertentu[11]. Angket atau kuesioner adalah teknik pengumpulan data di mana responden diberi serangkaian pertanyaan untuk dijawab. Teknik ini efisien dan efektif jika peneliti memiliki pemahaman yang jelas tentang variabel yang akan diukur dan kebutuhan responden[12]. Kuesioner berisi pertanyaan-pertanyaan yang telah dibuat oleh peneliti dan dijawab oleh responden. Kemudian, jawaban tersebut dikumpulkan dan diolah oleh peneliti sehingga menghasilkan kesimpulan.

III. Hasil dan Pembahasan

1. Pengumpulan Data

Pada penelitian ini menggunakan kuesioner sebagai metode pengumpulan data, Dimana kuesioner ini dibagikan oleh penelitti pada bulan Juni 2024. Peneliti berhasil mendapatkan 103 responden pada penyebaran kuesioner. Terdapat 10 pertanyaan yang dijawah oleh responden. Berikut ini merupakan data pertanyaan yang diajukan peneliti kepada responden.

Tabel 1.Pertanyaan Kuisioner

Nomor	Pertanyaan
P1	Apakah anda menggunakan Aplikasi Whatsapp (WA)?
P2	Apakah Anda menggunakan WhatsApp setiap hari?
P3	Apakah Anda sering menerima pesan dari nomor yang tidak dikenal di WhatsApp?
P4	Apakah Anda mengetahui tentang risiko keamanan informasi saat menggunakan WhatsApp?
P5	Apakah Anda mengetahui tentang risiko keamanan informasi saat menggunakan WhatsApp?
P6	Apakah Anda pernah menerima pesan Undangan Pernikahan APK melalui WhatsApp?
P7	Apakah Anda pernah membuka undangan APK yang diterima di WhatsApp?
P8	Apakah Anda pernah mengisi data pribadi pada Undangan APK?
P9	Apakah Anda mengalami gangguan setelah mengisi data pribadi pada Undangan APK?
P10	Apakah Anda pernah melaporkan Undangan APK mencurigakan yang diterima di WhatsApp?

2. Pengolahan Data

Tabel 2. Usia Responden

Usia	Persentase
17 – 22 Tahun	82,5%
23 – 30 Tahun	13,6%
31 – 39 Tahun	1,9%
40 Tahun keatas	1,9%

Mayoritas responden berada dalam rentang usia 17 – 22 tahun, mencerminkan kelompok pengguna muda yang aktif menggunakan teknologi dan media sosial. Kelompok usia ini cenderung lebih terhubung secara digital dan mungkin lebih rentan terhadap ancaman siber seperti malware “Undangan.APK”.

Tabel 3. Jenis Kelamin Responden

Jenis Kelamin	Persentase
Laki-laki	52,4%
Perempuan	48,5%

Pada tabel 3 Distribusi jenis kelamin hampir seimbang dengan sedikit lebih banyak responden laki-laki dibandingkan perempuan. Ini menunjukkan bahwa kesadaran dan perilaku keamanan informasi di WhatsApp tidak jauh berbeda antara laki-laki dan perempuan.

Tabel 4. Pekerjaan Responden

Pekerjaan	Persentase
Pelajar/Mahasiswa	83,5%
Pekerja Swasta	11,7%
PNS	1%
Wirausaha	2,9%
Guru	1%
Lainnya(Pelatihan,Mekanik)	2%

Pada tabel 4 Mayoritas responden adalah pelajar atau mahasiswa, yang lagi-lagi menunjukkan dominasi kelompok usia muda. Kelompok ini mungkin memiliki pengetahuan teknis yang baik, namun belum tentu memiliki kesadaran penuh terhadap risiko keamanan informasi.

Tabel 5. Pengguna Whatsapp

Pengguna Whatsapp	Persentase
YA	100%
TIDAK	0%

Pada tabel 5 Semua responden menggunakan WhatsApp, yang merupakan dasar penting untuk penelitian ini karena WhatsApp adalah platform

utama yang diteliti. Ini memastikan bahwa data yang dikumpulkan relevan dengan tujuan penelitian.

Tabel 6. Pengunaan Whatsapp

Penggunaan Whatsapp Setiap Hari	Persentase
YA	97,1%
TIDAK	2,9%

Pada tabel 6 Hampir semua responden menggunakan WhatsApp setiap hari, menunjukkan bahwa aplikasi ini merupakan bagian penting dari rutinitas harian mereka. Ini juga berarti bahwa risiko terpapar pesan phishing dan malware melalui WhatsApp sangat tinggi.

Tabel 7. Menerima Pesan

Menerima Pesan dari Nomor Tidak Dikenal	Persentase
YA	43,7%
TIDAK	56,3%

Pada tabel 7 Lebih dari separuh responden tidak menerima pesan dari nomor yang tidak dikenal, namun, persentase yang menerima pesan dari nomor tidak dikenal juga cukup signifikan. Inimenunjukkan adanya potensi risiko dari pesan yangtidak dikenal yang bisa mengandung malware atau phishing.

Tabel 8. Resiko Keamanan Informasi

Mengetahui Resiko Keamanan Informasi pada Whatsapp	Persentase
YA	76,7%
TIDAK	23,3%

Pada tabel 8 Sebagian besar responden menyadari risiko keamanan informasi saat menggunakan WhatsApp, meskipun masih ada yang tidak

menyadarinya. Ini menunjukkan adanya kesadaran yang cukup baik di kalangan pengguna namun perlu ditingkatkan lebih lanjut.

Tabel 9. Verifikasi Dua Langkah

Mengaktifkan Verifikasi Dua Langkah Whatsapp	Persentase
YA	53,4%
TIDAK	46,6%

Pada tabel 9 Lebih dari separuh responden telah mengaktifkan fitur verifikasi dua langkah di WhatsApp, yang merupakan langkah positif dalam meningkatkan keamanan akun mereka. Namun, masih ada sebagian yang belum memanfaatkan fitur ini.

Tabel 10. Menerima Pesan

Menerima Pesan Undangan.APK	Persentase
YA	38,8%
TIDAK	61,2%

Pada tabel 10 Sebagian besar responden tidak menerima pesan undangan APK, namun masih ada yang pernah menerima pesan tersebut,yang menunjukkan adanya risiko signifikan terkait penyebaran malware melalui pesan semacam itu.

Tabel 11 . Membuka “Undangan.APK”

Membuka Undangan.APK	Persentase
YA	7,8%
TIDAK	92,2%

Pada tabel 11 hanya sebagian kecil responden yang membuka undangan APK, yang menunjukkan bahwa sebagian besar pengguna waspada terhadap pesan yang mencurigakan. Ini adalah tanda positif dalam hal kesadaran keamanan.

Tabel 12. Mengisi Data Pribadi

Mengisi Data Pribadi Pada Undangan.APK	Persentase
YA	3,9%
TIDAK	96,1%

Pada tabel 12 Hanya sedikit responden yang mengisi data pribadi pada undangan APK, yang merupakan indikasi baik bahwa sebagian besar pengguna tidak terjebak dalam perangkap ini.

Tabel 13. Mengalami Gangguan

Mengalami Gangguan Setelah Mengisi Pada Undangan.APK	Persentase
YA	4,9%
TIDAK	95,1%

Pada tabel 13 Sangat sedikit responden yang mengalami gangguan setelah mengisi data pada undangan APK,menunjukkan bahwa dampak langsung dari insiden tersebut rendah. Namun,ini tetap menunjukkan bahwa ada risiko nyata.

Tabel 14. Melaporkan Chat

Melaporkan Chat Mencurigakan Kepada Whatsapp	Persentase
YA	27,2%
TIDAK	72,8%

Pada tabel 14 Sebagian besar responden tidak melaporkan pesan mencurigakan kepada WhatsApp, menunjukkan kurangnya tindakan terhadap ancaman keamanan yang dihadapi. Ini mengindikasikan bahwa edukasi mengenai pentingnya melaporkan insiden semacam itu perlu ditingkatkan.

3. Hasil Analisa

Dengan kuesnioner ini didapatkan hasil bahwa mayoritas pengguna Whatsapp merasa cukup aman menggunakan aplikasi tersebut, meskipun pemahaman mendalam tentang enkripsi dan kebijakan privasi masih terbatas. Sebanyak 15% responden pernah mengalami insiden keamanan, menunjukkan perlunya peningkatan fitur keamanan dan respons cepat terhadap insiden. Pengguna juga menginginkan fitur keamanan tambahan seperti otentikasi dua faktor dan notifikasi aktivitas mencurigakan. Oleh karena itu, Whatsapp dan Pemerintah perlu fokus pada edukasi pengguna tentang keamanan informasi, transparansi kebijakan privasi, dan peningkatan teknologi keamanan untuk memperkuat kepercayaan dan kenyamanan pengguna dalam menggunakan aplikasi.

4. Upaya Pencegahan

Berikut adalah edukasi beberapa Langkah mudah untuk mencegah serangan siber (Cybercrime) pada Whatsapp :

a) Gunakan Kata Sandi yang Kuat dan Unik

Kata sandi yang kuat menggunakan kombinasi huruf besar, huruf kecil, angka, dan simbol, sehingga sulit ditebak oleh peretas. Hindari penggunaan kata sandi yang sama di berbagai akun untuk mencegah kebocoran data jika salah satu akun Anda diretas.

b) Aktifkan Verifikasi Dua Langkah

Verifikasi dua langkah menambah lapisan keamanan dengan meminta kode tambahan yang dikirim ke ponsel atau email Anda, selain kata sandi. Ini membuat lebih sulit bagi peretas untuk mengakses akun Anda bahkan jika mereka mengetahui kata sandi Anda.

c) Perbarui Perangkat Lunak Secara Berkala

Pembaruan perangkat lunak sering kali mencakup perbaikan untuk kerentanan keamanan yang baru ditemukan. Dengan selalu memperbarui sistem operasi, aplikasi, dan perangkat lunak keamanan Anda, Anda memastikan bahwa perangkat Anda dilindungi dari ancaman terbaru.

d) Hati-Hati dengan Email dan Tautan Phising

Phishing adalah teknik penipuan untuk mencuri informasi pribadi melalui email atau situs palsu. Jangan klik tautan atau unduh lampiran dari pengirim yang tidak dikenal. Verifikasi sumber email sebelum memberikan informasi pribadi atau sensitif.

e) Gunakan Perangkat Lunak Keamanan

Perangkat lunak antivirus dan aplikasi keamanan membantu mendeteksi dan menghapus virus, malware, dan ancaman lainnya. Pilih perangkat lunak dengan ulasan positif dan reputasi baik untuk perlindungan yang lebih baik.

f) Atur Privasi dan Izin Aplikasi

Batasi akses aplikasi hanya pada informasi yang benar-benar diperlukan untuk fungsionalitasnya. Dengan mengatur izin aplikasi, Anda mengurangi risiko kebocoran data pribadi. Periksa pengaturan privasi secara berkala dan sesuaikan sesuai kebutuhan.

g) Cadangkan Data Secara Teratur

Menyimpan salinan data penting di lokasi terpisah, seperti layanan cloud atau perangkat

penyimpanan eksternal, memastikan data Anda aman dari serangan siber atau kerusakan perangkat. Lakukan pencadangan secara rutin untuk menjaga data tetap terkini.

h) Hindari Menggunakan Wifi Publik

Jaringan Wi-Fi publik sering kali tidak aman dan dapat disadap oleh peretas. Saat harus menggunakan Wi-Fi publik, hindari melakukan transaksi yang melibatkan informasi sensitif seperti login akun bank atau pembelian online. Gunakan VPN untuk mengenkripsi koneksi Anda dan menjaga data tetap aman.

i) Kenali Tanda-Tanda Malware dan Ransomware

Malware dan ransomware adalah jenis perangkat lunak berbahaya yang bisa mencuri data atau mengunci perangkat Anda hingga tebusan dibayar. Tanda-tanda infeksi termasuk performa perangkat yang melambat, munculnya pop-up mencurigakan, dan akses terbatas ke file. Jika Anda mencurigai adanya malware, segera jalankan pemindaian antivirus.

j) Terus Belajar dan Mengedukasi Orang Lain

Ancaman keamanan siber terus berkembang, sehingga penting untuk selalu mengikuti berita dan informasi terbaru tentang keamanan. Edukasi diri Anda melalui blog keamanan, berita teknologi, dan kursus online. Bagikan pengetahuan ini dengan keluarga dan teman untuk membantu mereka melindungi informasi pribadi mereka.

IV. Kesimpulan

Kesimpulan dari penelitian ini menunjukkan bahwa kesadaran pengguna terhadap risiko keamanan informasi masih perlu ditingkatkan. Meskipun sebagian besar responden menyadari risiko keamanan dan mengaktifkan fitur verifikasi dua langkah, masih ada sejumlah pengguna yang tidak waspada terhadap pesan mencurigakan, seperti "Undangan.APK". Temuan ini menunjukkan bahwa pengguna yang rentan masih menjadi target potensial bagi pelaku kejahatan siber yang menggunakan metode phishing dan malware untuk mencuri data pribadi.

Hasil penelitian ini juga menyoroti pentingnya edukasi berkelanjutan dan peningkatan fitur keamanan pada aplikasi WhatsApp. Pengguna membutuhkan lebih banyak informasi dan dukungan untuk memahami ancaman siber dan bagaimana melindungi diri mereka sendiri. Oleh karena itu, upaya kolaboratif antara penyedia layanan seperti WhatsApp dan pemerintah sangat penting untuk memberikan edukasi yang lebih baik dan memperkuat teknologi keamanan guna mengurangi risiko serangan siber dan menjaga informasi pribadi pengguna tetap aman.

V. Daftar Pustaka

[1] Erwin Ginting, Yolanda Eka Putri, Chairu Nisya, and Selly Febriyanti, "Kesadaraan Keamanan Informasi Data Pribadi Terhadap Pengguna Media Sosial," *1UNESJournal Inf. Syst.*, vol. 8, no. 1, pp. 1–8, 2023.

[2] Wahyuddin, Lutfiah Firdausiah Ersa, Gusti Aningsih, Taufik Hidayat, and Alem Febri Sonni, "Analisis Jaringan Komunikasi Penipuan Online Melalui Media Sosial Whatsapp Messenger," *J. Netnografi Komun.*, vol. 2, no. 2, pp. 33–50, 2024, doi: 10.59408/jnk.v2i2.27.

[3] S. A. Sudjayanti and D. Hamdani, "Digital Forensic Analysis Of APK Files In Phishing Scams On Whatsapp Using The NIST Method," vol. 4, no. 1, pp. 100–110, 2024.

[4] Artanti Zahra Adisa and Andriyanto Adhi Nugroho, "Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk," *Justisi*, vol. 10, no. 1, pp. 242–256, 2024, doi: 10.33506/js.v10i1.2980.

[5] M. N. P. Ma'ady, A. N. Zahra, M. Z. Darmawan, R. Abdillah, and P. Anaking, "Analisis Modus Penipuan Digital Teknik Phising melalui Aplikasi WhatsApp Menggunakan Metode BPMN (Studi Kasus Pada Peretasan E-Wallet)," *Semin. Nas. Sist. Inf.*, vol. 7, no. 1, pp. 3800–3806, 2023, [Online]. Available: https://jurnalfti.unmer.ac.id/index.php/senasif/article/view/469/417

[6] S. Khasanah and T. Sutabri, "Analisis Pencegahan Pencurian Data Melalui Aplikasi Whatsapp Menggunakan Metode Kriptografi," *J. Sain dan Tek.*, vol. 5, no. 2, pp. 145–153, 2023.

[7] G. Eka Sila and C. Mochamad Taufik, "Literasi Digital Untuk Melindungi Masyarakat Dari Kejahatan Siber," *Komversal*, vol. 5, no. 1, pp. 112–123, 2023, doi: 10.38204/komversal.v5i1.1225.

[8] Y. Arie Budi Suprio and M. Najib, "Analisa Dampak Kesadaran Keamanan Informasi Pengguna Aplikasi Whatsapp Terhadap Penyebaran Link Web Phising," *Semin. Nas. Corisindo*, pp. 318–322, 2022, [Online]. Available: https://corisindo.stikom-bali.ac.id/penelitian/index.php/semnas/article/view/65

[9] A. Abdul Wahid, "Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, no. November, pp. 1–5, 2020.

[10] Risdiana Chandra Dhewy, "Pelatihan Analisis Data Kuantitatif Untuk Penulisan Karya Ilmiah Mahasiswa," *J-ABDI J. Pengabdi. Kpd. Masy.*, vol. 2, no. 3, pp. 4575–4578, 2022, doi: 10.53625/jabdi.v2i3.3224.

[11] T. Nurrochman, R. Syafira, A. Sahata Sitanggang, I. Halim, P. Salsabina, and A. Aisy, "Analisis Yang Mempengaruhi Penggunaan M-Banking Bagi Nasabah BNI," *l Masharif al-Syariah J. Ekon. dan Perbank. Syariah*, vol. 7, no. August, pp. 559–566, 2022, doi: 10.30651/jms.v7i2.14216.

[12] B. Santoso, M. A. Ghofur, and J. Kuswanto, "Analysis of WhatsApp Mod User Awareness Information Security with Static Analysis Methods and Quantitative Methods," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 213–222, 2021, doi: 10.54706/senastindo.v3.2021.128.