PT Jurnal Cendekia Indonesia
Jurnal Sinergi Pengabdian Masyarakat
Homepage: https://journal.jci.co.id/jspm
Vol. 1 No. 1 (2025) pp: 25-30
P-ISSN: XXXX-XXXX, e-ISSN: XXXX-XXXX

Ancaman Tersembunyi: Risiko Virus pada Gambar Whatsapp dan Upaya Perlindungan Diri

[1]Gilang Rama Permana*, [2]Shadam Jodian Saputra, [3]Naufal Imam Hilmy, [4]Lutfi Nur Wahid, [5]Florida Virginia Luan, [6]Sopian Noer Mohamad

[1]Sistem Informasi, Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
[2]Sistem Informasi, Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
[3]Sistem Informasi, Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
[4]Sistem Informasi, Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
[5]Sistem Informasi, Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
[6]Sistem Informasi, Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia

[1]Unpamgilang@gmail.com*, [2]Shadamjodiansaputraa@gmail.com, [3]Nopal.wkt2@gmail.com, [4]Lutfinrwhd260702@gmail.com, [5]Viviluan436@gmail.com, [6]Sopiannur1999@gmail.com

Abstract

WhatsApp is one of the most widely used messaging applications because of its ease and speed in exchanging information, including image files. However, behind this convenience, there is a hidden threat in the form of malware insertion through image files. Cybercriminals often use steganography techniques to embed malicious code in images without changing their visual appearance. When the image is downloaded and opened, malware can be activated and attack the user's device. This article discusses the potential dangers of images on WhatsApp, virus insertion techniques, and protection strategies that can be carried out. The methods used are literature studies and analysis of real incidents, such as the case of the spread of Pegasus spyware. The findings show that low user awareness, automatic download habits, and the use of unofficial applications increase the risk. As a protective measure, users are advised to disable the automatic download feature, routinely update applications, use antivirus, and be careful with files from unknown sources. This article also emphasizes the importance of increasing digital security literacy and innovation in the development of automatic detection features on communication platforms. With a better understanding, users can take preventive steps against cyber attacks that are disguised through visual media.

***Keywords**: WhatsApp, Steganography, Image Virus, Cyber Security, User Protection.*

Abstrak

WhatsApp merupakan salah satu aplikasi perpesanan yang banyak digunakan karena kemudahan dan kecepatannya dalam bertukar informasi, termasuk file gambar. Namun, di balik kenyamanan tersebut, terdapat ancaman tersembunyi berupa penyisipan malware melalui file gambar. Pelaku kejahatan siber kerap memanfaatkan teknik steganografi untuk menanamkan kode berbahaya dalam gambar tanpa mengubah tampilannya secara visual. Ketika gambar tersebut diunduh dan dibuka, malware dapat diaktifkan dan menyerang perangkat pengguna. Pengabdian kepada masyarakat ini membahas potensi bahaya gambar di *WhatsApp*, teknik penyisipan virus, serta strategi perlindungan yang dapat dilakukan. Metode yang digunakan adalah studi pustaka dan analisis insiden nyata, seperti kasus penyebaran *spyware Pegasus*. Temuan menunjukkan bahwa lemahnya kesadaran pengguna, kebiasaan mengunduh otomatis, serta penggunaan aplikasi tidak resmi memperbesar risiko. Sebagai upaya perlindungan, pengguna disarankan untuk menonaktifkan fitur unduh otomatis, rutin memperbarui aplikasi, menggunakan antivirus, dan berhati-hati terhadap file dari sumber tidak dikenal. Pengabdian kepada masyarakat ini juga menekankan pentingnya peningkatan literasi keamanan digital serta inovasi dalam pengembangan fitur deteksi otomatis di platform komunikasi. Dengan pemahaman yang lebih baik, pengguna dapat mengambil langkah preventif terhadap serangan siber yang terselubung melalui media visual.

Kata Kunci: *WhatsApp*, Steganografi, Virus Gambar, Keamanan Siber, Perlindungan Pengguna.

A. PENDAHULUAN

Di tengah era digital yang saling terkoneksi, aplikasi pesan instan telah berkembang jauh melampaui fungsi awalnya sebagai alat komunikasi. *WhatsApp* kini menduduki posisi puncak sebagai platform dominan yang telah menjadi bagian tak terpisahkan dari aktivitas harian lebih dari dua miliar pengguna global. Peranannya tidak lagi terbatas pada komunikasi pribadi, melainkan telah merambah ke

Diterima Redaksi: 15-05-2025 | Selesai Revisi: 30-05-2025 | Diterbitkan Online: 30-06-2025

ranah kerja, pendidikan, transaksi bisnis informal, hingga penyebaran informasi publik. Dalam derasnya arus komunikasi ini, pertukaran media visual—khususnya gambar—mengalami lonjakan luar biasa, dengan estimasi mencapai miliaran file setiap harinya.

Rekayasa Sosial Menggunakan Gambar sebagai Umpan, ditambahkan acuan pada teori terkini dari Fischer dan Park (2021), yaitu Model Kerentanan Visual-Semantik (*Visual-Semantic Vulnerability Model*). Teori ini menjelaskan bahwa efektivitas manipulasi sosial melalui media gambar sangat bergantung pada kolaborasi antara elemen visual dan semantik. Visual yang dirancang meyakinkan—seperti logo resmi, kualitas tinggi, atau desain profesional—mampu meruntuhkan pertahanan awal pengguna dengan membangun kredibilitas instan. Ketika sikap skeptis telah melemah, pesan semantik yang bersifat membujuk seperti "Selamat, Anda menang hadiah!" atau "Akun Anda terancam!" menjadi lebih mudah diterima. Fischer dan Park menekankan bahwa semakin tinggi kredibilitas visual suatu gambar, semakin rendah ambang kepercayaan pengguna terhadap isi pesan tersebut, membuat mereka lebih mudah terjerat tindakan seperti mengklik tautan berbahaya.

Transisi dari komunikasi berbasis teks sederhana seperti SMS menuju komunikasi yang sarat dengan konten visual (*rich media)* menandai perubahan besar dalam pola interaksi manusia. Ketersediaan teknologi yang memudahkan pengambilan dan berbagi gambar telah memperkaya komunikasi sehari-hari. Namun, kemajuan ini juga memperluas permukaan serangan digital secara signifikan. Jika sebelumnya ancaman siber cenderung berasal dari lampiran email atau tautan mencurigakan, kini bahaya bisa bersembunyi di balik file gambar yang tampak biasa dan sering dibagikan tanpa curiga.

Secara kognitif, pengguna cenderung lebih waspada terhadap file berekstensi .exe, .apk, atau .zip karena diasosiasikan dengan aplikasi yang dapat dijalankan. Sebaliknya, file gambar seperti .jpg atau .png dipersepsikan sebagai media pasif yang aman untuk dilihat. Pandangan inilah yang dimanfaatkan oleh pelaku kejahatan siber. Mereka secara cerdas mengeksploitasi rasa aman yang keliru ini untuk merancang serangan yang lebih subtil, efisien, dan sulit dikenali oleh pengguna biasa.

Ancaman tersebut menjadi semakin penting untuk diperhatikan di Indonesia, negara dengan penetrasi internet seluler yang tinggi dan adopsi *WhatsApp* yang hampir merata di seluruh lapisan masyarakat. Di sini, *WhatsApp* telah menjadi infrastruktur utama dalam komunikasi sosial dan ekonomi—dari grup keluarga, komunitas lokal, hingga koordinasi pekerjaan profesional. Ketergantungan besar ini menjadikan pengguna Indonesia sebagai target empuk bagi penyebaran malware berskala besar yang memanfaatkan media gambar sebagai pintu masuk.

Meskipun *WhatsApp* dilengkapi dengan teknologi *enkripsi end-to-end* (E2EE) yang memastikan pesan hanya dapat dibaca oleh pengirim dan penerima, fitur ini membawa konsekuensi tersendiri. Karena konten pesan tidak bisa dipantau, maka file yang dikirim juga tidak dapat diperiksa keamanannya oleh sistem. Dengan demikian, tanggung jawab sepenuhnya berada di tangan pengguna untuk mengevaluasi apakah file yang diterima aman atau tidak.

Perluasan makna "*virus*" dalam konteks ini sangat penting. Sering kali istilah tersebut digunakan untuk menyebut berbagai bentuk perangkat lunak berbahaya (*malware*). Dalam gambar, ancaman tidak harus berupa virus yang menyebar, melainkan bisa berupa *spyware, ransomware, trojan*, atau bahkan gambar yang menyamar sebagai umpan untuk skema *phishing*.

Meskipun banyak penelitian telah menyoroti penyebaran *malware* lewat *email* dan situs *web*, serangan melalui file gambar di aplikasi pesan instan dengan enkripsi kuat masih belum banyak dibahas secara luas. Terdapat celah besar antara kecanggihan serangan yang terus berkembang dan rendahnya kesadaran keamanan pengguna. Celah inilah yang menjadikan vektor serangan ini sangat berbahaya dan layak menjadi perhatian utama.

Dengan latar belakang tersebut, Pengabdian kepada masyarakat ini memiliki dua tujuan utama. Pertama, untuk mengkaji secara mendalam aspek teknis dan psikologis dari penyebaran *malware* lewat gambar di platform seperti *WhatsApp*. Kedua, berdasarkan temuan tersebut, disusun strategi mitigasi yang praktis dan mudah diterapkan oleh berbagai kalangan. Pada akhirnya, Pengabdian kepada masyarakat ini menyimpulkan bahwa benteng pertahanan paling kuat bukan terletak pada teknologi canggih, melainkan pada literasi digital dan kebiasaan aman yang dibangun oleh penggunanya sendiri..

B. PELAKSAAAN DAN METODE

Kegiatan Pengabdian Kepada Masyarakat ini dilaksanakan melalui pendekatan kolaboratif dan edukatif yang menyasar warga Mushalla At-Taqwa, yang terletak di Jl. H. Rean RT.001/001, Kelurahan Benda Baru, Kecamatan Pamulang, Kota Tangerang Selatan. Kelompok sasaran terdiri dari pengguna aktif *WhatsApp* di lingkungan tersebut, termasuk kalangan remaja, ibu rumah tangga, serta tokoh-tokoh lokal.

Tahapan pelaksanaan kegiatan meliputi beberapa langkah utama, yakni:

1. Tahap Awal (Perencanaan)

Kegiatan diawali dengan identifikasi kebutuhan mitra melalui pengamatan langsung dan koordinasi dengan pengurus mushalla. Dalam fase ini, tim pelaksana menyusun rencana kegiatan, materi edukasi, serta media pendukung seperti modul pelatihan dan materi visual yang mudah dipahami oleh masyarakat awam.

2. Pemaparan Materi

Selanjutnya, dilakukan penyampaian informasi mengenai:

a. Bentuk-bentuk serangan siber yang dapat disisipkan dalam gambar digital.
b. Teknik penyembunyian kode jahat dalam file gambar menggunakan steganografi.
c. Potensi bahaya dari membuka file tidak dikenal.
d. Cara menjaga keamanan digital dalam penggunaan *WhatsApp* secara bijak.

Sesi ini dikemas dalam bentuk penyuluhan interaktif menggunakan alat bantu visual dan studi kasus nyata yang relevan.

3. Sesi Praktik Lapangan

Peserta dilatih langsung untuk melakukan langkah-langkah teknis, seperti:

a. Menyesuaikan pengaturan *WhatsApp* untuk mematikan unduhan otomatis.
b. Mengatur tingkat privasi dan keamanan yang optimal.
c. Mendeteksi file gambar yang mencurigakan.
d. Menginstal aplikasi keamanan seperti antivirus yang tersedia gratis.

Kegiatan ini dirancang agar peserta dapat mempraktikkan pengetahuan tersebut secara langsung melalui perangkat pribadi mereka.

4. Simulasi Situasi Nyata

Kegiatan dilanjutkan dengan skenario interaktif yang menghadirkan simulasi penerimaan file mencurigakan. Peserta diminta menilai dan merespons kasus tersebut sesuai dengan materi yang telah disampaikan. Tujuannya adalah melatih respons cepat dan logis terhadap potensi serangan digital.

5. Penilaian Hasil Kegiatan

Evaluasi dilakukan untuk mengetahui efektivitas kegiatan, dengan membandingkan tingkat pemahaman sebelum dan sesudah pelatihan. Umpan balik peserta juga dikumpulkan sebagai bahan pertimbangan dalam pengembangan kegiatan serupa di masa mendatang.

6. Program Lanjutan

Peserta diberi kesempatan untuk terus berinteraksi dan mendapatkan informasi lanjutan melalui grup *WhatsApp* yang dikelola oleh tim. Grup ini menjadi sarana berbagi materi tambahan dan tempat konsultasi seputar keamanan digital.

Metode yang digunakan merupakan perpaduan antara edukasi teoritis, praktik langsung, dan simulasi berbasis kasus. Pendekatan ini dirancang agar peserta tidak hanya memahami ancaman yang tersembunyi dalam file gambar digital, tetapi juga memiliki keterampilan nyata dalam mengatasinya.

Dengan penerapan metode ini, masyarakat di lingkungan Mushalla At-Taqwa diharapkan memiliki kesadaran digital yang lebih tinggi serta mampu menjaga diri dari risiko siber yang semakin kompleks dalam penggunaan media digital seperti *WhatsApp*.

Melalui pendekatan ini, kegiatan diharapkan mampu meningkatkan literasi keamanan siber masyarakat serta membentuk kebiasaan digital yang lebih aman dalam penggunaan aplikasi pesan instan seperti *WhatsApp*.

Sebelum kegiatan berlangsung, tim melakukan observasi lapangan serta berdiskusi dengan tokoh masyarakat dan pengurus mushalla. Hasil observasi menunjukkan bahwa sebagian besar warga aktif menggunakan *WhatsApp*, namun belum memahami risiko tersembunyi yang mungkin terkandung dalam file gambar. Banyak yang belum menyadari bahwa media gambar dapat dimanfaatkan sebagai sarana penyebaran malware.

Berdasarkan temuan tersebut, tim menyusun materi penyuluhan yang disesuaikan dengan kebutuhan masyarakat. Materi disampaikan dalam bentuk sederhana dan mudah dipahami, meliputi konsep dasar steganografi, contoh kasus penyebaran *malware* melalui gambar, pengenalan fitur keamanan pada *WhatsApp*, serta langkah-langkah pencegahan. Media pendukung meliputi modul cetak, slide presentasi, dan video edukatif singkat.

Kegiatan dimulai pukul 09.00 WIB dan dibuka oleh perwakilan pengurus mushalla. Penyuluhan dilaksanakan dengan pendekatan ceramah interaktif, mendorong peserta untuk terlibat aktif melalui sesi tanya jawab dan berbagi pengalaman. Narasumber menyampaikan materi menggunakan bahasa yang mudah dipahami agar pesan dapat diterima secara efektif oleh semua kalangan.

Setelah sesi penyuluhan, kegiatan dilanjutkan dengan praktik langsung. Peserta diminta mengecek dan menyesuaikan pengaturan keamanan pada *WhatsApp* mereka, menonaktifkan fitur unduh otomatis media, serta menginstal aplikasi antivirus ringan yang direkomendasikan. Tim mendampingi peserta secara langsung, terutama mereka yang kurang familiar dengan fitur teknologi, seperti warga lanjut usia.

Selama praktik, peserta juga diberikan pemahaman tentang cara mengenali file gambar yang mencurigakan, seperti ukuran file yang tidak normal, file yang tidak dapat dibuka, atau file yang memicu unduhan aplikasi tertentu. Contoh nyata seperti kasus *spyware Pegasus* juga disampaikan sebagai pembelajaran.

Kegiatan diakhiri dengan evaluasi dan diskusi terbuka. Peserta menyampaikan pendapat dan pemahaman mereka setelah mengikuti pelatihan, serta mengisi kuesioner singkat untuk mengukur peningkatan pengetahuan. Hasilnya menunjukkan peningkatan signifikan dalam

pemahaman peserta terhadap ancaman digital yang tersembunyi dalam gambar.

Sebagai bentuk keberlanjutan, peserta diberikan akses terhadap materi digital dalam format PDF serta tautan ke video edukatif. Peserta juga didorong untuk menyebarkan informasi tersebut kepada keluarga dan lingkungan sekitar guna menciptakan efek edukatif berantai di masyarakat.

Metode pelaksanaan kegiatan mengedepankan prinsip partisipatif, komunikatif, dan praktis. Masyarakat tidak hanya sebagai penerima informasi, tetapi juga dilibatkan secara aktif dalam proses pembelajaran dan penerapan. Diharapkan pendekatan ini dapat meningkatkan kesadaran dan ketangguhan digital masyarakat dalam menghadapi ancaman siber.

C. HASIL DAN PEMBAHASAN

Kegiatan Pengabdian Kepada Masyarakat (PKM) dengan tema "Ancaman Tersembunyi: Risiko Virus pada Gambar *WhatsApp* dan Upaya Perlindungan Diri" telah sukses dilaksanakan di Mushalla At-Taqwa yang berlokasi di Jl. H. Rean RT.001/001, Kelurahan Benda Baru, Kecamatan Pamulang, Kota Tangerang Selatan. Program ini bertujuan untuk meningkatkan literasi digital masyarakat, khususnya dalam mengenali potensi bahaya yang tersembunyi dalam file gambar yang dikirim melalui aplikasi *WhatsApp*.

Acara diawali dengan sambutan resmi dari dosen pembimbing, Ibu Mufidah Karimah, S.Kom., M.Kom., yang menekankan pentingnya kesadaran masyarakat terhadap aspek keamanan digital sebagai bagian dari kehidupan era informasi. Sambutan tambahan juga disampaikan oleh Ketua Kegiatan Dakwah Mushalla (KDM) Mushalla At-Taqwa, yang mengapresiasi inisiatif mahasiswa dalam memberikan kontribusi nyata kepada masyarakat sekitar.

Gambar 1 Pembukaan Kegiatan PKM

Kegiatan ini diketuai oleh Gilang Rama Permana sebagai ketua tim, didampingi oleh anggota Shadam Jodian Saputra, Naufal Imam Hilmy, Lutfi Nur Wahid, Florida Virginia Luan, dan Sopian Noer Mohamad. Seluruh tim bekerja sama dalam menyusun kegiatan dengan pendekatan yang komunikatif dan mudah dipahami oleh peserta dari berbagai latar usia dan latar belakang.

Gambar 2 Anggota PKM

Materi pertama yang disampaikan membahas secara khusus mengenai ancaman tersembunyi pada file gambar di platform *WhatsApp*. Para peserta diberikan pemahaman mengenai modus penyebaran malware melalui media gambar, serta risiko yang dapat timbul apabila file dibuka sembarangan. Penyampaian materi dilakukan secara visual dan interaktif untuk mempermudah pemahaman.


Gambar 3 Diskusi

Selanjutnya, peserta diarahkan untuk melakukan praktik langsung menggunakan perangkat masing-masing. Mereka dibimbing dalam menonaktifkan fitur unduhan otomatis, mengatur privasi akun, serta mengaktifkan fitur keamanan seperti verifikasi dua langkah di aplikasi *WhatsApp*. Pendekatan praktikal ini membantu peserta memahami langkah-langkah proteksi secara nyata dan langsung.

Untuk mengasah kemampuan respons peserta, dilaksanakan simulasi situasi nyata. Peserta diberikan skenario menerima file gambar dari kontak tak dikenal yang berpotensi mengandung virus. Mereka dilatih untuk mengambil langkah yang aman, seperti tidak membuka file, memblokir pengirim, dan melaporkannya sebagai spam. Simulasi ini menjadi latihan penting untuk membentuk kewaspadaan digital.

Tim pengabdian juga memperluas wawasan peserta dengan menjelaskan jenis file lain yang rentan terhadap serangan siber, seperti file .exe, .apk, dan dokumen yang

mengandung makro. Pengetahuan ini disampaikan agar peserta dapat lebih waspada terhadap beragam jenis ancaman digital, tidak hanya terbatas pada file gambar semata.

Pendekatan humanis turut menjadi kunci keberhasilan kegiatan ini. Tim pengabdian memberikan pendampingan intensif kepada peserta yang kurang terbiasa dengan teknologi, termasuk peserta lanjut usia. Hal ini menciptakan suasana pembelajaran yang inklusif serta mendorong kolaborasi antar generasi dalam membangun kesadaran akan keamanan digital.

Hasil kegiatan menunjukkan adanya peningkatan pemahaman yang signifikan. Sebelum pelatihan, hanya sebagian kecil peserta yang menyadari risiko dari file gambar berbahaya. Namun setelah pelatihan, mayoritas peserta tidak hanya mampu mengidentifikasi risiko, tetapi juga mampu menerapkan langkah-langkah pengamanan digital secara mandiri.

Tingginya antusiasme peserta terlihat dari keterlibatan aktif mereka selama diskusi. Banyak di antara mereka yang mengajukan pertanyaan, berbagi pengalaman pribadi, bahkan menyarankan adanya kegiatan lanjutan terkait topik keamanan digital lainnya. Sebagai bentuk tindak lanjut, dibentuklah grup *WhatsApp* khusus untuk memfasilitasi komunikasi dan edukasi lanjutan antar peserta dan tim pengabdian.

Gambar 4 Penyerahan Plakat

Sebagai penutup kegiatan, tim menyerahkan plakat kepada pengurus Mushalla At-Taqwa sebagai bentuk penghargaan atas dukungan yang diberikan. Selain itu, seluruh peserta menerima sertifikat partisipasi. Momen akhir ditandai dengan sesi foto bersama antara peserta, tim pengabdian, dosen pembimbing, dan pengurus mushalla, yang menjadi simbol sinergi antara akademisi dan masyarakat dalam meningkatkan ketahanan digital komunitas.

Gambar 5 Foto Bersama Kegiatan PKM

Ucapan Terima Kasih

Kami menyampaikan apresiasi kepada Ibu Mufidah Karimah, S.Kom., M.Kom., selaku dosen pembimbing dari Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Pamulang, atas dukungan dan arahannya selama persiapan hingga pelaksanaan kegiatan. Ucapan terima kasih juga kami sampaikan kepada pengurus Mushalla At-Taqwa dan pengurus masjid setempat atas dukungan fasilitas yang telah diberikan, serta kepada teman-teman anggota PKM yang telah bekerja sama dengan penuh semangat dan dedikasi. Kami juga menghaturkan terima kasih kepada warga dan masyarakat sekitar yang telah berpartisipasi secara aktif. Semoga edukasi yang telah diberikan dapat diterapkan dan disebarluaskan lebih luas di lingkungan masing-masing.

E. DAFTAR PUSTAKA

Andress, J. (2021). Cybersecurity: The beginner’s guide. Packt Publishing.

Casey, E. (2019). Digital evidence and computer crime: Forensic science, computers and the Internet (3rd ed.). Academic Press.

Chai, C. A. (2023). Peningkatan kesadaran keamanan digital melalui literasi siber di masyarakat perkotaan. Jurnal Keamanan Informasi dan Teknologi, 9(2), 87–95.

Gasser, U., Maclay, C., & Palfrey, J. (2010). Working towards a deeper understanding of digital safety for children and young people in developing nations. Berkman Center Research Publication.

Hakim, A. R., & Sutrisno, E. (2021). Ancaman malware pada media sosial dan upaya pencegahannya. Jurnal Teknologi Informasi dan Komunikasi, 12(1), 45–53.

Kaspersky. (2023). Malware in image files: How hackers hide viruses in photos. Retrieved from https://www.kaspersky.com

Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing. Wiley.

McFedries, P. (2022). Protecting your privacy online. Que Publishing.

Oktaviani, T., & Prasetyo, R. (2022). Pentingnya literasi digital dalam menghadapi ancaman siber di era komunikasi digital. Jurnal Komunikasi Digital Indonesia, 4(3), 112–121.

Pavur, J. (2020). Image-based malware attacks on WhatsApp: Mechanisms and mitigations. Proceedings of the International Conference on Cybersecurity and Privacy.

Putri, Y. D., & Nugroho, B. (2020). Perlindungan data pribadi di era digital: Studi kasus WhatsApp. Jurnal Hukum dan Teknologi, 5(2), 73–80.

Quinn, M. J. (2020). Ethics for the information age (8th ed.). Pearson.

Rouse, M. (2022). Image steganography and malware infiltration. SearchSecurity by TechTarget. Retrieved from https://www.techtarget.com/searchsecurity

Schneier, B. (2020). Secrets and lies: Digital security in a networked world (2nd ed.). Wiley.

Sharma, A., & Grover, S. (2019). Cyber hygiene awareness and practices among mobile app users. International Journal of Cyber Security and Digital Forensics, 8(1), 34–40.

Sobari, A. (2021). WhatsApp sebagai media komunikasi dan potensi ancaman siber. Jurnal Sistem Informasi, 9(2), 56–65.

Stiawan, D., Idris, M. Y. I., & Abdullah, J. (Eds.). (2018). Recent advances in intrusion detection systems for cybersecurity. Springer.

Syahrir, D., & Fauzi, M. (2022). Strategi pencegahan malware berbasis sosial media di kalangan remaja. Jurnal Ilmu Komputer dan Teknologi Informasi, 15(3), 101–108.

Symantec. (2023). Cyber threat report: Malware trends and defenses. NortonLifeLock.

Widodo, H., & Pramudito, R. (2021). Pengaruh literasi digital terhadap kesadaran keamanan data pribadi. Jurnal Literasi Digital Indonesia, 3(2), 88–97.