International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 Mar 2025

ANALYZING PHISING CAMPAIGNS WITH SOC TOOLS

N.Madhu Bhavani[1], Bonu Swetha Devi Sai Priya[2], Mekapothula Ganesh[3], Emmidi Shivaraj[4], Balne Shivak Umar[5]

[1] Associate Professor, Dept. of CS, Sri Indu College of Engineering and Technology, Hyderabad,

[2 3 4] Research Student, Dept. of CS Sri Indu College of Engineering and Technology, Hyderabad

Abstract**:** *The increasing cases of online fraud through the WhatsApp application in Indonesia are still very often found among the general public. The theft of privacy data through WhatsApp social media in the form of URLs or links, PDF invitation files is the impetus for this research. Therefore, further handling is needed through security management so that the fraud can be resolved properly. This scam is very common, to protect users from phishing attacks, it is necessary to understand the mode of phishing on WhatsApp and develop better security methods. Phishing threats are a common type of online fraud that often occurs through WhatsApp Messager. This research uses a qualitative analysis method using data collection through literature studies. The purpose of this research is to collect and review more literature on the topic, as well as to investigate and analyze the various types of Phishing threats that occur through the WhatsApp application. The results of this study show that phishing has become one of the most important security threats related to the WhatsApp application. Phishing occurs when someone impersonates an official organization or a well-known figure to trick users into trusting messages sent to the perpetrator. Users are instructed to download a program file in apk or pdf format by the scammer.*

Keyword: *Phishing Threats, Phishing Analysis*

Abstrak: Meningkatnya kasus penipuan online melalui aplikasi WhatsApp di indonesia masih sangat sering kita temukan dikalangan masyarakat pada umumnya. Pencurian data privasi melalui media sosial WhatsApp dalam bentuk URL atau link, file undangan PDF menjadi pendorong penelitian ini. Oleh karena itu, diperlukan penanganan lebih lanjut melalui manajemen sekuriti agar penipuan tersebut dapat terselesaikan dengan baik. Penipuan ini sangat umum sekali, untuk melindungi pengguna dari serangan Phising, perlu adanya pemahaman mengenai modus Phising di WhatsApp dan pengembangan metode keamanan

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

yang lebih baik. Acaman Phising adalah jenis penipuan online umum yang sering terjadi melalui WhatsApp Messager. Penelitian ini menggunakan metode analisis kualitatif dengan menggunakan pengumpulan data melalui studi literatur. Tujuan dari penelitian ini adalah untuk mengumpulkan dan meninjau lebih lanjut literatur mengenai topik tersebut, serta untuk menyelidiki dan menganalisis dari berbagai jenis ancaman Phising yang terjadi melalui aplikasi WhatsApp. Hasil penelitian ini menunjukan bahwa Phising telah menjadi salah satu ancaman keamanan paling utama yang berkaitan dengan aplikasi WhatsApp. Phising terjadi ketika seseorang menyamar sebagai sebuah organisasi resmi atau figur terkenal untuk mengelabui penggunanya agar mempercayai pesan yang dikirimkan kepada si pelaku. Pengguna diinstruksikan untuk mengunduh file program dalam format apk atau pdf oleh penipu.

Kata Kunci: Ancaman Phising, Analisis Phising

PENDAHULUAN

Revolusi digital telah mengubah cara individu dalam berinteraksi. Sebelum era digital, komunikasi banyak bergantung pada media tradisional seperti surat, telepon, atau pertemuan langsung yang sering kali membutuhkan waktu dan biaya yang tidak sedikit. Namun kemajuan teknologi digital telah merombak cara-cara tersebut, menciptakan berbagai platform dan alat komunikasi yang lebih cepat, efisien, dan mudah diakses. Salah satunya adalah penggunaan aplikasi WhatsApp. WhatsApp menjadi salah satu aplikasi pesan yang paling banyak digunakan, baik untuk komunikasi pribadi ataupun bisnis (Isadora K., Aqila N.P., et al., 2024). WhatsApp memperkenalkan banyak fitur tambahan yang memungkinkan penggunanya dapat melakukan interaksi secara online melalui pengiriman pesan, panggilan suara, dan video. Kemudahan inilah yang menjadikan WhatsApp sebagai media yang menjadi sebuah pilihan banyak orang.

Dalam era digital, aplikasi instan pesan berupa WhatsApp ini telah mendominasi disetiap negara dan menjadi bagian integral dalam komunikasi sehari-hari. Tetapi berbagai macam ancaman keamanan pun juga turut serta mengintai disetiap aktivitas online kita dalam WhatsApp, salah satu yang sering terjadi adalah Phising. Kepopuleran WhatsApp sebagai media interaksi mengundang banyak perhatian para pelaku kejahatan *cyber* yang menganggap aplikasi WhatsApp ini sebagai ladang untuk melakukan kejahatan Phising. Phising sendiri berasal dari kata *fishing* yang berarti memancing, yang merupakan salah satu upaya untuk mendapatkan informasi data seseorang seperti kata sandi dan data pribadi dengan samaran yang mengatasnamakan identitas serta entitas yang dapat dipercaya atau *legitimate organization* dan biasanya berkomunikasi secara elektronik (Arhani I., 2024).

Berbagai platform, termasuk media sosial, situs web, dan juga aplikasi dapat menjadi sasaran empuk pelaku kejahatan siber Phising tersebut. Situs web Phising ini menjadi suatu kejahatan yang dirancang untuk *wallhacker* dan dibuat sedemikian rupa supaya menyamai dengan aslinya. Dalam WhatsApp, penjahat siber mencoba mengirim pesan ke nomor tertentu. Pesan ini mungkin berisi informasi berupa *file* atau *link* penipuan. Ada yang mengirimkan undangan pernikahan berupa *file* PDF dan ada juga yang mengirimkan link bahwa nomor ini telah dipilih sebagai pemenang undian. Ketika pengguna mendownload atau menekan *link* tersebut, mereka diminta untuk mengkonfirmasi melalui link tersebut. Pengguna akan dibawa ke situs web berbahaya yang telah dimodifikasi oleh pelaku. Cara kerja Phising bermula dari pelaku (*phisher*) akan menghubungi kepada korban dan berpura-pura berasal dari bisnis yang sah seperti bank, telepon atau penyedia layanan internet melalui email, media sosial, telepon, atau pesan SMS. Pelaku pun juga bisa membuat seolah-olah undangan pernikahan tersebut nyata, dan ketika dibuka *file* PDF tersebut, maka akan ada pemberitahuan bahwa *file* tersebut berbahaya. Tetapi jika orang tersebut tetap mengklik *file* tersebut, maka perangkatnya dapat rusak dan data pribadinya akan dicuri oleh pelaku. Pengetahuan pengguna yang minim tentang

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

penggunaan alat teknologi informasi adalah yang mendorong Phising dapat terjadi (Lokapala Y.H., Nurfauzi F.J., et al., 2024).

Kejahatan Phising bisa terjadi dimana saja dan kapan saja, dalam aplikasi WhatsApp sudah tidak heran apabila terjadi kejahatan Phising ini. Jadi, dihimbau bagi pengguna harus selalu waspada dalam menggunakan aplikasi WhatsApp ini. Minimnya pengetahuan yang cukup untuk mengakses berbagai macam aplikasi internet dan oknum-oknum yang tidak bertanggung jawab mencoba memanfaatkan pengguna WhatsApp tersebut. Ketidaktahuan tersebut membuat pengguna aplikasi WhatsApp terjerumus dalam korban tindakan kejahatan siber. Oleh karenanya, saat menerima pesan yang tidak diketahui berasal dari siapa, pengguna harus memastikan kembali dan melihat keakuratan pesan yang diterimanya. Pengguna harus selalu mengkoreksi bahwa pesan yang dikirimkan oleh orang yang tidak dikenal tersebut benar atau tidak melalui situs-situs resmi dan jangan mudah percaya jika didapati menerima informasi berupa file PDF yang tidak jelas kebenarannya atau sebuah link penipuan. Karena bisa saja hal tersebut sangat berbahaya yang dapat mengancam keselamatan perangkat dan juga pengguna (Putra I.K.O.K., Darmawan I.M.A., et al., 2022)

Pengguna WhatsApp tentunya merasa khawatir dengan maraknya kejahatan siber *Phising* ini. Maka dengan demikian, manajemen data membutuhkan penggunaan manajemen sekuriti untuk menanggulangi masalah ini (Ningrum D.A., Fauzi A., et al., 2023). Keamanan adalah kunci terpenting untuk melakukan kegiatan komunikasi dalam WhatsApp karena sebagian info dan aktivitas komunikasi dilakukan secara *online*. WhatsApp membutuhkan keamanan yang canggih untuk memastikan keamanan data-data pengguna dapat terjaga dan terhindar dari serangan siber *Phising* tersebut. Manajemen sekuriti adalah metode sistematis untuk mengidentifikasi, menganalisis, dan memitigasi resiko yang mungkin mempengaruhi organisasi atau individu. Manajemen sekuriti menjadi penting dalam aplikasi WhatsApp untuk melindungi pengguna dari berbagai ancaman kejahatan dunia maya. Oleh karena itu, diperlukan adanya analisis manajemen keamanan ancaman kejahatan siber pada aplikasi WhatsApp. Resiko yang mungkin terjadi meliputi serangan *malware, Phishing*, peretasan akun, pencurian identitas, dan penyebaran informasi palsu. Untuk memitigasi resiko ini, praktik manajemen sekuriti yang efektif harus diterapkan. Berdasarkan permasalahan diatas untuk menunjang penelitian yang relevan dan mengkaji permasalahan dengan baik, maka penelitian ini difokuskan ke beberapa masalah yang akan dikaji.

Berdasarkan latar belakang di atas, maka rumusan masalah yang menjadi fokus penelitian ini, sebagai berikut:

1. Mengapa pengguna Aplikasi WhatsApp harus mengembangkan strategi keamanan yang lebik baik untuk melindungi pengguna dari serangan *Phising*?
2. Apa peran edukasi dan kesadaran keamanan digital terhadap pengetahuan pengguna dalam resiko penanganan kejahatan *Phising*?
3. Apa peran manajemen sekuriti dalam Aplikasi WhatsApp untuk mencegah terjadinya kejahatan *Phising*?
4. Bagaimana efektivitas manajemen sekuriti dapat melindungi privasi dan keamanan pengguna?

METODE

Penelitian ini menggunakan metode deskriptif kualitatif. Penelitian deskriptif kualitatif merupakan jenis penelitian ilmiah yang bertujuan untuk menjelaskan fenomena yang sedang terjadi. Meliputi aktivitas, perubahan, sifat, hubungan, persamaan, dan perbedaan antar fenomena. Dengan kata lain, penelitian deskriptif kualitatif berfokus pada subjek penelitian melalui Teknik pengumpulan data seperti survei perpustakaan, sehingga memungkinkan terciptanya tanggapan terhadap peristiwa terkini.

Pendekatan yang akan digunakan dalam penelitian ini yaitu Tinjauan Pustaka. Tinjauan Pustaka merupakan merupakan kegiatan analisis yang berupa kritik terhadap makalah

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

penelitian tentang topik tertentu dalam suatu bidang akademik. Isi tinjauan pustaka ini berupa penjelasan atau pembahasan mengenai temuan atau teori topik penelitian. Penjelasan teori-teori tersebut dapat dijadikan landasan teori dalam penulisan karya ilmiah dan melakukan kegiatan penelitian. Selain itu, penelitian yang dilakukan dapat merupakan pengembangan dari penelitian sebelumnya atau dapat juga merupakan penelitian yang pertama kali dilakukan.

Penelitian ini menerapkan tinjauan terhadap literatur yang relevan untuk mendalami dan memahami keamanan yang sangat rentan terhadap *Phising* melalui aplikasi WhatsApp dan bagaimana langkah manajemen sekuriti yang telah diusulkan dan diterapkan sebelumnya. Pengumpulan data dari studi kasus yang telah mengalami permasalahan sama adalah cara peneliti untuk menganalisis kasus-kasus dan memahami modus *Phising* yang umum digunakan oleh penyerang serta bagaimana kesuksesan dalam implementasi manajemen sekuriti.

Tabel 1. Penelitian terdahulu yang relevan

No	Judul	Penulis	Tujuan Penelitian	Hasil Dan Kesimpulan
1.	"Ancaman phishing terhadap pengguna sosial media dalam dunia Cyber Crime"	Mia haryati wibowo, nur fatimah	Tujuan penelitian untuk membahas apa psihing dan cara menanggulangi phishing pada sosial media	Pada penelitian tersebut dijelaskan bahwa banyak dari pengguna whatsaap tidak memikirkan ancaman phising, salah satu serangan yang di luncurkan oleh penjahat siber itu dengan menaruh fake link pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan pengguna.
2.	"Analisis modus phising terhadap whatsapp"	Kaela isadora, Nashwa putri aqila, Hermia gustina, Azarine nabila, nurfitriana	Tujuan penelitian ini untuk menganalisis modus phising yang terjadi melalui whatsapp, melalui metode yang akan digunakan oleh penjahat siber.	Pada penelitian ini di jelaskan bagaiamana strategi kejahatan phising melalui whatsaap, akan menyebabkan korban tertipu dan secara tidak langsung membocorkan informasi pribadi yang dapat merugikan korban. Biasanya, phising dilakukan oleh penipu dengan cara mengirim pesan palsu yang mengatasnamakan suatu institusi atau pihak resmi.
3.	"Aplikasi Whatsapp Bajakan sebagai Ancaman Kejahatan Siber di Indonesia"	Angelia Pratiwi Mastiurlani Christina Sitorus	bertujuan untuk menyajikan pemahaman yang mendalam tentang fenomena tersebut dan memberikan kesimpulan yang didasarkan pada konteks hukum yang relevan	Penggunaan situs media sosial seperti Line, Facebook, Telegram, Blackberry Massanger, WhatsApp, dan platform lainnya telah menjadi kegiatan umum di masyarakat, yang dipengaruhi oleh kemajuan teknologi informasi. Seiring dengan perkembangan media sosial, terjadi perubahan dalam pola perilaku masyarakat

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

				terkait budaya, etika, dan norma yang diterima. Privasi menjadi isu krusial bagi individu dan lembaga yang terlibat dalam interaksi dengan orang lain atau institusi lainnya.
4.	"Analisis manajemen risiko ancaman kejahatan siber (Cyber Crime) dalam aplikasi whatsapp"	Reni kuswulandari, Axzara wirid isra jowanka, Telaga nabila putri riyanto, Titin listiani	Tujuan penelitian ini untuk melihat dan menganalisis praktik manajemen risiko berupa ancaman kejahatan dunia maya pada penggunakan whatsapp.	Pada penelitian ini penulis menganalisis manajemen risiko terhadap ancaman kejahatan siber dalam aplikasi whatsapp menjadi suatu kebutuhan yang mendesak. Risiko yang mungkin terjadi mencakup serangan malware, phishing, peretasan akun, pencurian data pribadi, dan penyebaran informasi palsu, dalam rangka mengurangi risiko ini, praktik manajemen risiko yang efektif perlu diimplementasikan.
5.	"Analisis kejahatan Cyber Crime pada peretasan dan penyadapan aplikasi whatsapp"	Nurul Khasanah, Tata Sutabri	Tujuan penelitian ini untuk menganalisis terkait kejahatan cybercrime pada peretasan dan penyadapan aplikasi WhatsApp.	Pada Penelitian ini peretasan merupakan suatu perbuatan atau pembobolan terkait jaringan, sistem, komputer tanpa adanya izin dari pengguna. Cybercrime ialah kejahatan yang dilakukan melalui media virtual yang bisa dilakukan oleh teknologi cyber dan dapat dikategorikan sebagai tindakan criminal.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

6.	"Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong)" (2024)	Dhafin Naufal Ayman, Lucky Nurhadiyanto	bertujuan untuk menjelaskan fenomena yang sedang berlangsung. Termasuk aktivitas, perubahan, sifat, hubungan, kesamaan, dan perbedaan antara fenomena.	Kejahatan siber di Indonesia memiliki sejarah yang Panjang. Kejahatan siber di Indonesia pertama kali terjadi pada tahun 1983, Ketika teknologi komputer dan internet masih dalam tahap pengembangan. Pada saat itu, kejahatan siber di Indonesia berupa penyalahgunaan komputer untuk melakukan kegiatan illegal berupa pencurian data dan penggelapan uang melalui sistem komputer
7	"Digital Forensic Analysis Of APK Files In Phishing Scams On Whatsapp Using The NIST Method. (2024)"	Shafa Alya Sudjayanti, Dani Hamdani	Penelitian ini bertujuan untuk memberikan wawasan dalam mencegah dan memitigasi penipuan phishing melalui file APK di WhatsApp Android. Ini juga menyoroti pentingnya langkah-langkah keamanan siber yang kuat.	Melalui analisis forensik menggunakan metode NIST dan dengan menerapkan teknik rekayasa balik, penelitian ini telah menganalisis struktur dan mekanisme kerja file APK. Penelitian ini berhasil mengidentifikasi skema serangan, menganalisis kode APK yang digunakan, dan memahami mekanisme kerja dan tujuan dari aplikasi yang berpotensi berbahaya ini.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

8.	"ANALISIS JARINGAN KOMUNIKASI PENIPUAN DARING MELALUI MEDIA SOSIAL WHATSAPP MESSENGER"	Wahyuddin, Lutfiah Firdausiah Ersa, Gusti Aningsih, Taufik Hidayat, Alem Febri Sonni5	Tujuan Penelitian Ini ingin menunjukan bahwa pelaku utama penipuan daring melalui WhatsApp Messenger adalah penjahat yang juga menjadi aktor utama. Phishing dan sniffing adalah dua jenis penipuan online yang sering terjadi menggunakan WhatsApp.	Pada Penelitian ini penulis menemukan bahwa Pelaku kejahatan memanfaatkan aplikasi WA untuk melakukan tindak penipuan online. Salah satu bentuk penipuan yang sering di gunakan pelaku kejahatan melalui WA adalah phising. Tindakan phising terjadi dikarenakan pelaku mengatasnamakan instansi resmi bahkan nama pejabat, menggunakan link, icon bergambar, melalui kontak para tokoh masyarakat agar pelaku mendapatkan tingkat kepercayaan yang tinggi bagi para pengguna sehingga korban percaya dengan pesan yang diterima
9.	"Analisis Kejahatan Phising dengan Modus Link Undangan Pernikahan Pada Aplikasi WhatsApp: Perspektif Hukum Pidana Ekonomi"	Fairus Hasna	Tujuan penelitian ini untuk menunjukkan bahwa regulasi yang ada belum sepenuhnya efektif dalam menangani kejahatan Phising dan diperlukan strategi penegakan hukum yang lebih komprehensif untuk mengatasi kendala yang ada.	Pada Penelitian ini menunjukan bahwa Penegakan hukum terkait tindak pidana Phising dengan modus Link undangan di Indonesia menghadapi berbagai kendala signifikan. Pertama, kendala hukum dan regulasi menjadi hambatan utama, Kedua, kendala teknis dan teknologi turut memperumit penegakan hukum. Ketiga, kesadaran dan literasi digital masyarakat yang masih rendah juga menjadi tantangan dari penulis.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

10.	"Analisis Modus Penipuan Digital Teknik Phising melalui Aplikasi WhatsApp Menggunakan Metode BPMN (Studi Kasus Pada Peretasan E-Wallet)"	Mochamad Nizar Palefi Ma'ady, Aisyah Nabila Zahra, Muhammad Zidan Darmawan, Rosyid Abdillah, Purnama Anaking	Tujuan penelitian ini untuk menunjukan bagaimana penipu menggunakan teknik phishing untuk mencuri data pribadi korban dan bagaimana upaya untuk melindungi diri dari serangan phishing.	Pada penelitian ini penulis menemukan bahwa phishing tidak hanya disebarkan melalui pesan singkat atau email palsu yang mengatasnamakan institusi tertentu saja. Teknik phishing yang dilakukan oleh para pelaku kejahatan siber juga semakin berkembang dengan memanfaatkan kecanggihan teknologi untuk mengelabui korbannya. Salah satu contohnya yaitu maraknya pengiriman file seperti, pdf, atau .apk yang berisikan malware. File-file jenis ini dikirimkan melalui media sosial, seperti whatsapp dan dikemas sedemikian rupa dengan pesan yang meyakinkan sehingga, file tersebut terlihat aman dan resmi dari sebuah institusi atau organisasi yang sah
11.	Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Review Metode Studi Literatur	M. Wildan Alvian Prastya, Muhlis Tahir, Ayu Agustyas Ningrum, Aqiqul Putra Zaibintoro, Lumatus Sa'adah, Ummi Mutmainnah, Sabella Kalimatus Sa'diah.	Tujuan dari penelitian ini adalah untuk mengumpulkan dan meninjau literatur tentang topik ini, untuk menyelidiki dan menganalisis berbagai jenis ancaman phishing yang terjadi melalui aplikasi WhatsApp.	Hasil penelitian ini menunjukkan bahwa phishing telah menjadi salah satu ancaman keamanan utama, terutama berkaitan dengan aplikasi WhatsApp.
12.	Analisis Penyadapan pada Aplikasi WhatsApp Menggunakan Sinkronisasi Data	Safrizal Dian, Gustina, Nurul Aisyah, Arman Syah Putra, V.H Valentino, Budhi Sriyono Prasetyo.	Tujuan penelitian ini adalah bagaimana mencegah dari penyadapan WhatsApp yang dilakukan oleh orang yang tidak bertanggung jawab sehingga pada penelitian ini dapat diketahui setelah celah apa saja dan apa saja yang harus dilakukan jika ingin mencegah hal tersebut.	Penyadapan pada whatsapp adalah salah satu bentuk cybercrime yang merugikan karena pelaku penyadapan bisa mengetahui apa isi whatsapp korban penyadapan. Ini sangat berbahaya karena jika isi whatsapp korban berisi hal-hal penting maka pelaku bisa saja melakukan tidakan criminal yang lain karena mengetahui ada hal penting yang terdapat di whatsapp korban.

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

13.	Analisis Kesadaran Keamanan Terhadap Ancaman Phishing	Nunu Vadila, Ahmad R. Pratama	Penelitian ini bertujuan untuk melakukan penilaian terhadap tingkat kesadaran masyarakat terhadap ancaman phishing.	Hasil dari penelitian ini diharapkan bisa dimanfaatkan untuk menjadi pembelajaran kedepannya sehingga bisa meningkatkan kesadaran terhadap ancaman phishing
14.	Perlindungan Korban Kejahatan Penipuan Online Bermodus Apk(Android Package Kit) melalui Whatsapp	Aldin Aliyyu Hakim, Dian Alan Setiawan	Penelitian ini bertujuan untuk mengetahui perlindungan hukum terhadap korban kejahatan penipuan dengan modus APK (Android Package Kit) melalui WhatsApp ditinjau dari Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.	Hasil penelitian menyatakan bahwa perlindungan hukum terhadap korban kejahatan penipuan online dengan modus APK melalui WhatsApp bersifat preventif yang bertujuan untukpencegahan dan represif yang bertujuan untuk penindakan.
15.	Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phising	I Kadek Odie Kharisma Putra, I Made Adi Darmawan, I Putu Gede Juliana, Indriyani	Phising adalah jenis penipuan dunia maya yang bertujuan mencuri akun korban. Tentu saja, sebagian besar kejahatan dunia maya biasanya dimulai dengan phising, sehingga pengguna internet harus selalu waspada.	Kejahatan siber dengan metode phising seringkali ditemukan pada platform media sosial. Media sosial menjadi sasaran utama hacker untuk menjalankan aksinya karena media sosial memiliki banyak pengguna dan sangat bebas tanpa adanya suatu filter.
16.	Analisis Bibliometrik Mengenai Serangan Phishing dan Whatsapp menggunakan Vosviewer	Rafi Kurnia Sujiwana, Achmad Fahmi Ainur Ridho, Dwi Cindy Aryanti, Nur Aini Rakhmawati4	mengenai serangan phising di aplikasi whatsapp bertujuan untuk memperoleh hubungan antara phishing dan whatsapp dengan mendeteksi berbagai titik koneksi yang dihasilkan dalam jaringan pemetaan kata kunci	keyword “phishing” pada penelitian yang terpublikasi memiliki hubungan yang sangat erat dengan keamanan dan Whatsapp. Terdapat penelitian yang menyoroti banyaknya kasus serangan phishing yang terjadi di whatsapp. Oleh karena itu, sosialisasi mengenai edukasi sangat penting dalam mengatasi ancaman kejahatan siber salah satunya phishing.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

17.	Analisis Penyadapan Pada Aplikasi Whatsapp Dengan Menggunakan Metode Sinkronisasi Data	Yusuf Andi Putra, Tata Sutabri	jurnal ini adalah pengguna whatsapp versi manapun bisa lebih aman dalam menggunakan whatsapp karena bisa mengetahui celah keamanan yang dimiliki whatsapp sehingga bia lebih berhati hati	pengembangan jurnal ini, adalah kita harus berhati hati dalam memakai sosial media karena jika tidak digunakan secara hati-hati maka hp kita bisa disadap oleh pelaku kejahatan cyber yang dapat merugikan kita. Dengan adanya sinkronisasi data maka harus hati-hati lagi Bagaimana jika data kita tersinkron dengan sosial media, atau media internet dengan adanya hal tersebut maka hal tersebut menjadi salah satu yang harus kita perhatikan.
18.	Pelatihan Mengamankan Akun Whatsapp Dari Peretasan	Reza Maulana, Septian Rheno Widianto,Nurmalasari, Lady Agustin Fitriana	Tenaga pengajar pada Yayasan Pondok Pesantren Mu'thasim Billah sebagian besar menggunakan layanan aplikasi WhatsApp.	Perkembangan teknologi yang semakin meningkat membuat penggunaan teknologi di dunia juga semakin meningkat dan memberi dampak yang baik maupun buruk terhadap keamanan informasi yang ada.
19.	Analisis kejahatan online phising pada institusi pemerintah/ pendidik sehari-hari	Purnamasari, Tata Sutabri	Menangkap hanya akun pengguna dan kata sandi, bertujuan untuk mengeksploitasi data pengguna dan administrator.	jahatan dunia maya (CyberCrime) merupakan tindakan yang berupa kriminal dimana jaringan komputer atau komputer menjadi alat, sasaran atau lokasi utnuk kejahatan. Baik menyerang fasilitas publik maupun milik pribadi. Phising adalah memancing untuk mengumpulkan kata sandi atau password.

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

20.	Pelatihan Mengamankan Akun Whatsapp Dari Peretasan	Reza Maulana, Septian Rheno Widianto, Nurmalasari, Lady Agustin Fitriana	Tujuan yang ingin dicapai dalam pengabdian masyarakat ini adalah memberikan edukasi dan pelatihan dengan memanfaatkan fitur aplikasi WhatApp untuk kemananan data dari para hacker	Perkembangan teknologi yang semakin meningkat membuat penggunaan teknologi di dunia juga semakin meningkat dan memberi dampak yang baik maupun buruk terhadap keamanan informasi yang ada. Sistem keamanan dan privasi WhatsApp sering kali menjadi target peretasan oleh orang-orang yang tidak bertanggung jawab. Padahal, bisa dipastikan bahwa sistem keamanan aplikasi chatting yang satu ini tentu tinggi.

HASIL DAN PEMBAHASAN

Bentuk Pengembangan Strategi Keamanan Manajemen Sekuriti Dalam Mencegah Terjadinya Phising Dalam Aplikasi WhatsApp

Melakukan improvisasi pada manajemen sekuriti dalam mencegah terjadinya Phising menjadi perhatian utama dimana seperti yang diketahui, keamanan aplikasi WhatsApp masih

sangat lemah dan rentan sekali dengan kejahatan siber. Manajemen sekuriti memiliki peran krusial dalam menjaga keamanan perusahaan dengan mengelola resiko yang terkait. Tanggung jawab mereka yakni meliputi penetapan kebijakan keamanan yang jelas, identifikasi potensi ancaman dan kerentanan, serta pengelolaan resiko dengan menerapkan kontrol keamanan yang tepat (Irawan, C. R., Fauzi, A., et al, 2024).

Setiap proses berjalannya aplikasi WhatsApp dukungan teknis keamanan sangat diperlukan. Permasalahan terhadap kejahatan Phising pada aplikasi WhatsApp belum dapat diatasi dan tidak teratur. Pengamanan siber adalah langkah-langkah dan praktik yang dilakukan untuk melindungi data dari serangan dan ancaman kejahatan Phising. Dalam konteks aplikasi WhatsApp, sebagai aplikasi besar, penting untuk memiliki keamanan siber yang kuat untuk melindungi data sensitif, informasi operasional, dan infrastruktur teknologi yang digunakan dalam operasinya (Cahyani, A. D., Soesanto, E., Rahma, N. H., & Ramdan, M., 2023). Peran dan tanggung jawab manajemen sekuriti dalam mengelola resiko keamanan sangat penting dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi serta sumber daya perusahaan. Manajemen sekuriti juga berperan dalam manajemen resiko perusahaan. Dengan mengidentifikasi, mengevaluasi, dan mengelola resiko yang terkait dengan keamanan informasi dan operasional, manajemen sekuriti dapat membantu perusahaan untuk mengurangi potensi kerugian dan meningkatkan efisiensi dalam menjalankan operasional sehari-hari (Marfiana, 2020) dalam (Irawan, C. R., Fauzi, A., et al, 2024).

Pencegahan yang dapat dilakukan antara lain, memiliki kebijakan dan prosedur yang memadai untuk penggunaan teknologi informasi. Manajemen sekuriti dapat membantu perusahaan mengelola resiko keamanan secara efektif dengan fokus pada identifikasi ancaman, evaluasi resiko, dan strategi mitigasi ancaman digital. (Sitorus, M. G. B., Maria, N., & Safa, Y. N., 2024).

Kemampuan Peningkatan Keamanan Dasar Bagi Pengguna WhatsApp Dalam Mencegah Phising

Berbagai hal dapat menyebabkan ancaman *Phising* muncul diantaranya yaitu, kurangnya kesadaran dan pemahaman masyarakat tentang tindakan kejahatan Phising, penggunaan taktik Phising yang disesuaikan dengan lokasi pengguna untuk meningkatkan keberhasilan penipuan, penipuan *Phising* melalui media seperti WhatsApp terus menjadi ancaman yang harus diwaspadai oleh masyarakat, kekurang waspadaan masyarakat terhadap tanda-tanda *Phising* seperti email atau pesan yang tidak dikenal, tautan yang tidak dikenal, atau permintaan informa. Masyarakat dapat lebih waspada dan berhati-hati dalam melindungi data pribadi mereka dari Phising dengan memperoleh pemahaman yang lebih baik tentang komponen ini. (Prastya, M. W. A., Tahir, M., et al, 2024).

Elemen yang berkontribusi terhadap keberhasilan upaya *Phising*. Pertama-tama, penyebab utama *Phising* adalah ketidaktahuan pengguna internet terhadap keamanan informasi, khususnya di kalangan ibu rumah tangga dan remaja. Selain itu, upaya *Phising* menjadi semakin kompleks karena penyerang menggunakan teknik rekayasa sosial untuk menargetkan demografi pengguna tertentu, termasuk orang lanjut usia, yang kurang paham teknologi atau lebih rentan terhadap penipuan *online* karena mereka tidak menyadari bahaya yang ditimbulkan oleh dunia maya. Serangan Phising juga berhasil karena kesalahan manusia atau kurangnya kesadaran. Peringatan keamanan sering kali diabaikan oleh pengguna, sehingga memudahkan upaya *Phising* berhasil. Penyerang *Phising* menyesatkan pengguna agar membocorkan informasi pribadi dengan menggunakan teknik rekayasa sosial, seperti mempermainkan emosi, seperti rasa takut (Prastya, M. W. A., Tahir, M., et al, 2024).

Penyebab utama pengguna menjadi korban serangan *phishing* juga karena ketidaktahuan mereka terhadap informasi tentang kejahatan *Phising*. Hal ini termasuk tidak dapat membedakan nama domain asli dan palsu, tidak memperhatikan tanda keamanan browser, dan tidak mengetahui cara menangani upaya *Phising*. Kewaspadaan dan pemahaman yang

mendalam sangat diperlukan untuk dapat mencegah ancaman tersebut agar terhindar dari pelanggaran *Phising*. Dengan pemahaman yang lebih baik, diharapkan pengguna WhatsApp dapat lebih berhati-hati lagi dari serangan *Phising* yang merugikan. Tidak hanya waspada saja, edukasi mengenai *Phising* sangat penting. Pembaruan tentang teknik *Phising* yang sedang marak terjadi harus diketahui oleh pengguna. Mengurangi kemungkinan *Phising* dapat dilakukan dengan berbagi pengetahuan tentang keamanan siber dan melaporkan aktivitas atau akun yang mencurigakan.

Pentingnya Peran Manajemen Sekuriti Terhadap Keamanan Pengguna Dalam Aplikasi WhatsApp

Untuk menjaga ketersediaan, kerahasiaan, dan integritas data dan sumber daya perusahaan, manajemen sekuriti memainkan peran penting dalam mengendalikan ancaman keamanan. Manajemen sekuriti juga mencakup manajemen resiko. Melalui proses menemukan, menilai, dan mengendalikan ancaman keamanan informasi dan operasional, manajemen sekuriti dapat membantu dalam menurunkan kemungkinan kerugian dan meningkatkan efisiensi operasional. Peraturan yang sudah dibentuk oleh *platform* adalah satu upaya pendekatan dengan pengguna agar dapat terhindar dari hal yang tidak diinginkan seperti kejahatan *Phising*. Tetapi, pengguna tidak hanya harus mematuhi peraturan yang dibuat oleh platform dan pihak berwenang, namun mereka juga harus berpartisipasi secara aktif dalam menciptakan lingkungan media sosial yang aman.

Pihak berwenang dan aplikasi WhatsApp berkolaborasi dalam prosedur manajemen sekuriti untuk mengidentifikasi, menggagalkan, dan menegakkan tindakan hukum terhadap penjahat dunia maya. Selain itu, upaya sedang dilakukan untuk mendeteksi akun palsu yang sering digunakan oleh penipu untuk melakukan serangan *Phising*. Diyakini bahwa dengan mengadopsi pendekatan menyeluruh dan kolaboratif, kita dapat menciptakan lingkungan siber yang lebih aman dan lebih tahan terhadap serangan *Phising* yang lebih kompleks di dunia digital saat ini. Secara keseluruhan, hal ini menunjukkan bahwa mencegah upaya *Phising* pada aplikasi WhatsApp memerlukan pendekatan kepolisian berbasis tim yang menyeluruh. Inisiatif teknis dan hukum sangatlah penting, begitu pula taktik peningkatan kesadaran pengguna. Untuk menjaga internet lebih aman dan terlindungi dari meningkatnya bahaya *Phising*, pemerintah, perusahaan yang bersangkutan, dan masyarakat umum harus bekerja sama (Prastya, M. W. A., Tahir, M., et al, 2024).

Bentuk Pemahaman Tanda-tanda Phising Untuk Meningkatkan Privasi dan Keamanan Pengguna Aplikasi WhatsApp

Kejahatan *Phising* melalui koneksi obrolan WhatsApp memerlukan upaya tidak jujur, di mana pelaku berupaya berpura-pura sebagai sumber terpercaya untuk mendapatkan informasi keuangan atau informasi pribadi korban. Pengguna tentunya memerlukan pengetahuan dan kesadaran akan gejala-gejala serangan kejahatan *Phising* ini (Hasanudin, A. F., & Babussalam, A. B., 2024). Adapun uraian identifikasi masalah kejahatan phising melalui link chat WhatsApp yakni:

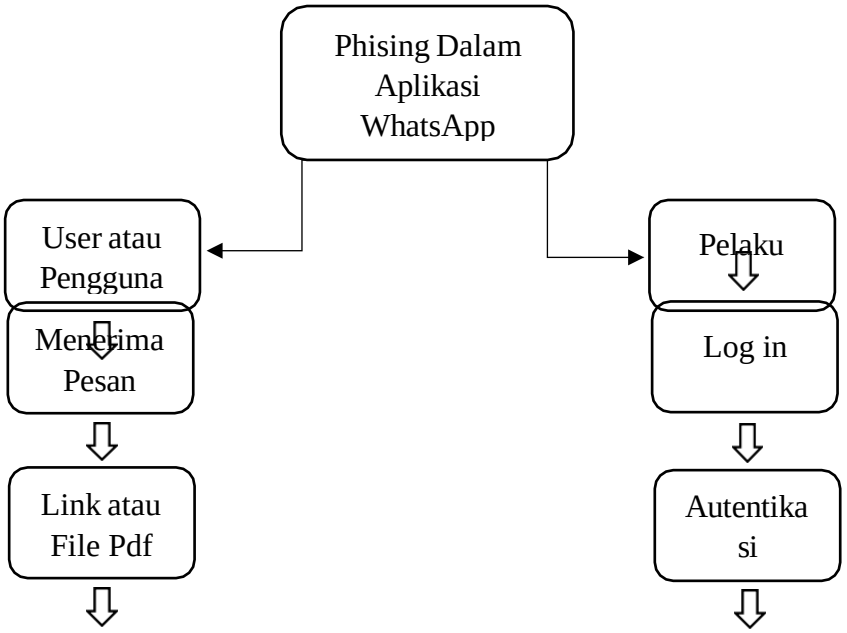
1. Tautan yang mencurigakan: Sebelum mengeklik tautan yang terkirim seharusnya pastikan dulu bahwasanya link yang terkirim pada chat WhatsApp itu aman yakni dengan memeriksa tautan yang diberikan, karena kejahatan *phissing* sendiri sering menggunakan URL palsu atau modifikasi kecil pada URL resmi sehingga tautan yang sekirannya mencurigakan dapat dihindari.
2. Pesan menekan atau darurat: Sebuah pesan yang dimana seolah-olah meyakinkan terus-terusan terhadap penerima pesan agar dapan menekan apa yang dikirim oleh pelaku phissing sehingga dapat diwaspadai pesan yang menciptakan urgensi atau tekanan. Seperti ancaman yang mengancam penonaktifan akun ataupun ada masalah keamanan yang

International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025

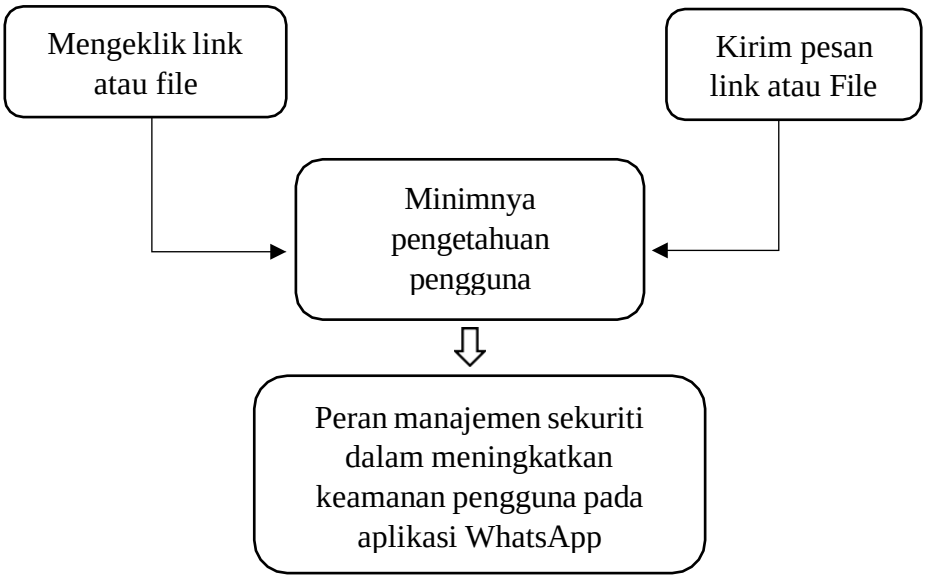
mendesak, pelaku Phising sering kali menggunakan taktik seperti ini agar korban tampak panik dan dapat melakukan apa yang diperintah oleh pelaku.

3. Permintaan informasi pribadi: *Phising* sering kali mengirimkan pesan ataupun tautan yang meminta agar penerima pesan dapat mengirimkan identitasnya sebagai data pelaku untuk melakukan tindakan kejahatan *Phising*, jika penerima pesan chat terdapat pesan seperti ini setidaknya penerima pesan tidak mengirimkan identitas pribadinya terlebih yang telah meminta informasi pribadi yang sensitif melalui tautan yang dikirim kechat WhatsApp.
4. Bahasa dan tata bahasa yang mencurigakan: Waspadai dan telitih bahasa yang digunakan dalam menerima pesan jika terdapat bahasa yang tidak biasa atau kesalahan tata bahasa dalam pesan yang dikirimkan. *Phising* sering kali memanfaatkan ketidak jelasan ataupun kesalahan dalam pengiriman pesannya dan itu bertujuan untuk mengecoh korban agar korban melakukan apa yang diperintah dari pesan chat yang disampaikan.
5. Verifikasi logo dan grafis: Jika pengirim pesan terdapat mencantumkan logo atau grafis perusahaan pada profilnya pastikan dulu bahwa chat yang masuk itu benar dan dijamin keasliannya dan tidak dimanipulasi. *Phisher* sering juga menggunakan taktik ini untuk mencoba meniru elemen desain untuk menipu korban phissing.
6. Penyamaran URL dengan *Hyperlink:* Jika tautan disematkan dalam kata-kata tertentu dapat diperhatikan terlebih dahulu bahwa URL yang sebenarnya mungkin akan terlihat berbeda dari apa yang ditampilkan. *Hover mouse* diatas tautan untuk melihat URL yang sebenarnya dan dapat terdeteksi mana yang asli dan mana yang palsu.
7. Pesan yang tidak biasa dari kontak yang dikenal: Jika pesan yang dikirim tidak biasa atau dapat dicurigai dari isi pesannya dari kontak yang sudah dikenal perlu adanya verifikasi keasliannya dengan cara menghubungi perngirim pesan secara terpisah sebelum mengambil tindakan yang diinginkan.
8. Penggunaan teknologi rekayasa sosial: *phisher* sering kali menggunakan teknik rekayasa sosial seperti halnya memanipulasi emosi atau menciptakan suatu alasan yang mendesak untuk meningkatkan peluang korban memberikan informasi kepada pelaku kejahatan phissing melalui chat whatsapp tersebut sehingga secara tidak langsung korban telah mengirimkan informasi kepada pelaku.

Conceptual Framework



International journal of imaging science and engineering
ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 Mar 2025



Gambar 1. ***Conceptual Framework***

Kerangka pemikiran diatas dalam artikel tersebut diperoleh melalui rumusan masalah, fakta, dan berbagai sumber lainnya:

Khasanah N., & Sutabri T. (2023). Analisis Kejahatan Cybercrime Pada Perentasan Dan Penyadapan Aplikasi Whatsapp . *Blantika: Multidisciplinary Journal*, 1(2): 44-45.

KESIMPULAN

Aplikasi whatsapp ini banyak digunakan untuk berkomunikasi, meskipun efisien, aplikasi ini juga rentan terhadap serangan phising, terutama pada modus berbasis *link*. Pada kejahatan *phising* ini kurangnya pemahaman sistem keamanan digital, sehingga banyak pengguna whatsapp terjebak oleh pesan palsu yang tampak sah. Pada penelitian ini menemukan bahwa pengguna whatsapp ini rendah pengetahuan keamanan sehingga meningkatnya resiko kebocoran data pribadi, sebab pengguna tidak selalu mengenali bahaya link palsu. Pada kesimpulan penelitian ini, disarankan juga untuk meliputi edukasi keamanan bagi pengguna untuk tanda phising, penguatan pada fitur keamanan whatsapp seperti autentikasi dua faktor dan deteksi otomatis *link*, serta menerapkan manajemen sekuriti yang efektif. Selain itu, disarankan dengan adanya sistem kerjasama pada penyedia layanan masyarakat dan platform media sosial untuk meningkatkan keamanan digital pada pengguna.

REFERENSI

Abrar, M. F., & Nasution, M. I. P. (2024). Analisis Peningkatan Keamanan Data Two Step Verification pada Aplikasi Whatsapp Messenger. *Surplus: Jurnal Ekonomi dan Bisnis*, *2*(2), 335-340.

Aliyyu Hakim, A., & Alan Setiawan, D. (2024). Perlindungan Korban Kejahatan Penipuan Online Bermodus Apk (Android Package Kit) melalui Whatsapp. *Jurnal Riset Ilmu Hukum*, *4*(1), 23–28. https://doi.org/10.29313/jrih.v4i1.3778

Andi Putra, Y., & Sutabri, T. (2023). Analisis Penyadapan Pada Aplikasi Whatsapp Dengan Menggunakan Metode Sinkronisasi Data. *Blantika : Multidisciplinary Journal*, *2*(1), 11–20. https://doi.org/10.57096/blantika.v2i1.8

Arahap A. D., Juardi D., & Irawan A. S. Y. (2024). Rancang Bangun Sistem Pendeteksi Link Phising Menggunakan Algoritma Random Forest Berbasis Web. *Jurnal Informatika dan Teknik Elektro Terapan*, 12(3).

Arhani I. (2024). Sanksi Pelaku Tindak Pidana Cyber Phising Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. In I. Arhani. UIN (Universitas Islam Negeri).

Ayman, D. N., & Nurhadiyanto, L. (2024). Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp (Studi Kasus Kurir Paket Bodong). *IKRA-ITH HUMANIORA: Jurnal Sosial dan Humaniora*, *8*(2), 373-384.

Azhari F., Sumarno S., Fauzi A., et al. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-Wallet. *Jurnal Kewirausahaan dan Multi Talenta*, 2(2): 138-147.

Cahyani, A. D., Soesanto, E., Rahma, N. H., & Ramdan, M. (2023). Manajemen Sekuriti: Pengamanan Objek Vital Pada PT. Nusa Halmahera Minerals. *Madani: Jurnal Ilmiah Multidisiplin*, 1(5).

Dian Nurdiansyah, Yonetta Deandra Anindira, Salwa Sihab Muhibin, & Alfina Haqqani Putri. (2023). Sosialisasi Digital Security Dalam Meningkatkan Edukasi Bermedia Digital Di Lingkungan Masyarakat Depok Baru. *Karunia: Jurnal Hasil Pengabdian Masyarakat Indonesia*, *2*(1), 109–120. https://doi.org/10.58192/karunia.v2i1.597

Ersa L. F., Aningsih G., et al. (2024). Analisis Jaringan Komunikasi Penipuan Online Melalui Media Sosial WhatsApp Messenger. *Netnografi Komunikasi*, 2(2): 73-90.

Firmansyah, P. D., Fauzi, A., Barja, R., Mulyana, A. P., Putri, T. N., Surachman, A., & Ramadhan, G. (2024). Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan. *Jurnal Kewirausahaan dan Multi Talenta*, *2*(2), 112-125.

Haryati W. M., & Nur F. (2017). Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *Jurnal of Education and Information Communication Technology*, 1(1).

Hasanudin, A. F., & Babussalam, A. B. (2024). Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking. *Jurnal Gagasan Hukum*, 6(01), 16-29.

Hasna, F. Analisis Kejahatan Phising dengan Modus Link Undangan Pernikahan Pada Aplikasi WhatsApp: Perspektif Hukum Pidana Ekonomi.

Irawan, C. R., Fauzi, A., et al. (2024). Pengaruh Efektivitas Manajemen Sekuriti Dalam Keamanan Perusahaan. Jurnal Ilmu Multidisplin. *Jurnal Ilmu Multidisplin*, 3(1), 59-68.

Isadora K., Aqila N. P., et al. (2024). Analisis Modus Phising Whatsapp. *Jurnal Akuntansi, Bisnis, dan Ekonomi Indonesia (JABEI)*, 3(2): 45-52.

Kadek Odie Kharisma Putra, I., Made Adi Darmawan, I., Putu Gede Juliana, I., Kunci, K., & Crime, C. (2022). Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phising Criminal Acts in the Digital World With a Form of Phishing. *CyberSecurity Dan Forensik Digital*, *5*(2), 77–82.

Khasanah N., & Sutabri T. (2023). Analisis Kejahatan Cybercrime Pada Perentasan Dan Penyadapan Aplikasi Whatsapp . *Blantika: Multidisciplinary Journal*, 1(2): 44-45.

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.

Lim, W. H., Liew, W. F., Lum, C. Y., & Lee, S. F. (2020). *Phishing Security: Attack, Detection, and Prevention Mechanisms*. 143–150. https://doi.org/10.56453/icdxa.2020.1017

Lokapala Y.H., Nurfauzi F.J., et al. (2024). Aspek Yuridis Kejahatan Phising dalam Ketentuan Hukum di Indonesia . *Indonesian Journal Of Criminal Law and Criminology (IJCLC)*, 5(1): 19-24.

Maulana, R., Widianto, S. R., Nurmalasari, N., & Fitriana, L. A. (2023). Pelatihan Mengamankan Akun Whatsapp Dari Peretasan. *Jurnal Penelitian Dan Pengabdian Masyarakat Jotika*, *2*(2), 31–34. https://doi.org/10.56445/jppmj.v2i2.68.

Ningrum D.A., Fauzi A., et al. (2023). Peran Manajemen Sekuriti Terhadap Keputusan Pembelian pada Pengguna Aplikasi Shopee (Studi Pustaka Manajemen Sekuriti). *Jurnal Ilmu Manajemen Terapan*.

Nova S. D., Soesanto E., et al. (2023). Analisis dan Pengembangan Sistem Manajemen Sekuriti Pada PT. Denso Manufacturing Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, 9(13): 225-236.

Prastya, M. W. A., Tahir, M., et al. (2024). Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Review Metode Studi Literatur. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 7(3), 190-197.

Putra I.K.O.K., Darmawan I.M.A., et al. (2022). Tindakan Kejahatan Pada Dunia Digital Dalam Bentuk Phising. *CyberSecurity dan Forensik Digital*, 5(2): 77-82.

Putra, Y. A., & Sutabri, T. (2023). Analisis Penyadapan pada Aplikasi Whatsapp Dengan Menggunakan Metode Sinkronisasi Data. *Blantika: Multidisciplinary Journal*, *1*(2), 132-141.

Safrizal, S., Gustina, D., Aisyah, N., Putra, A. S., Valentino, V. H., & Prasetyo, B. S. (2022). Analisis Penyadapan pada Aplikasi WhatsApp Menggunakan Sinkronisasi Data. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, *6*(1), 28–34. https://doi.org/10.55886/infokom.v6i1.453

Saputra F., Soesanto E., et al. (2024). Penerapan Manajemen Sekuriti Terhadap Cyber Crime di Kominfo. *IJM: Indonesian Journal of Multidisciplinary*, 2(1).

Sari, P., & Sutabri, T. (2023). Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari. *Jurnal Digital Teknologi Informasi*, *6*(1), 29. https://doi.org/10.32502/digital.v6i1.5620.

Sitorus A. P. M. C., & Astono A. (2024). Aplikasi WhatsApp Bajakan Sebagai Ancaman Kejahatan Siber di Indonesia. *Arus Jurnal Sosial dan Humaniora*, 4(1): 157-162.

Sitorus, M. G. B., Maria, N., & Safa, Y. N. (2024). Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek: Identifikasi, Evaluasi, dan Mitigasi Ancaman. *Jurnal Manajemen Informatika (JAMIKA)*, 14(2), 187-198.

Soyemi, J., & Hammed, M. (2020). an Enhanced Authentication Scheme for Preventing Phishing Attacks on Whatsapp Accounts. *Proceedings of the 2nd International Conference*, 102–108.

Sudjayanti, S. alya, & Hamdani, D. (2024). Digital Forensic Analysis Of APK Files In Phishing Scams On Whatsapp Using The NIST Method. *Brilliance: Research of Artificial Intelligence*, *4*(1), 100–110. https://doi.org/10.47709/brilliance.v4i1.3800.

Sujiwana, R. K., Ridho, A. F. A., Aryanti, D. C., & Rakhmawati, N. A. (2024). Analisis Bibliometrik Mengenai Serangan Phishing dan Whatsapp menggunakan Vosviewer. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, *8*(1), 101–105. https://doi.org/10.55886/infokom.v8i1.880.

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber Di Era Digital. *Journal of Business And Entrepreneurship*, *11*(1), 23. https://doi.org/10.46273/jobe.v11i1.365.

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, *2*(9), 864-870.

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2), 1–4.

Wildan Alvian Prastya, M., Tahir, M., Agustyas Ningrum, A., Putra Zaibintoro, A., Sa, L., Mutmainnah, U., Kalimatus Sa, S., Trunojoyo Madura, U., Raya Telang, J., Kamal, K., Bangkalan, K., Timur, J., & Pos, K. (2024). Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Review Metode Studi Literatur. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *7*(3), 190–197.