Jurnal Akuntansi, Bisnis dan Ekonomi Indonesia
Vol. 3 No. 2, 2024 hal. 45-52. https://akuntansi.pnp.ac.id/jabei
Jurusan Akuntansi Politeknik Negeri Padang, ISSN 2829-9043 (media online)

Analisis Modus Phising terhadap Whatsapp

Kaela Isadora[1], Nashwa Putri Aqila[2], Hermia Gustina[3], Azarine Nabila[4], Nurfitriana[5]

[1] Jurusan Akuntansi, Universitas Muhammadiyah Riau, 230301150@student.umri.ac.id
[2] Jurusan Akuntansi, Universitas Muhammadiyah Riau, 230301155@student.umri.ac.id
[3] Jurusan Akuntansi, Universitas Muhammadiyah Riau, 230301158@student.umri.ac.id
[4] Jurusan Akuntansi, Universitas Muhammadiyah Riau, 230301177@student.umri.ac.id
[5] Jurusan Akuntansi, Universitas Muhammadiyah Riau, nurfitri@umri.ac.id

Keywords:
Phishing, Whatsapp, Scammer, Previous Sources, Links

Received : 31 Juli 2024
Accepted : 14 Agustus 2024
Published : 31 Agustus 2024

ABSTRACT

We examine phishing attempts on WhatsApp in this study. This study's primary goal is to detect fraudulent activities by deceiving targets into stealing personal information from WhatsApp users. This study employs a descriptive methodology that draws on strategies from earlier works. Phishing is the practice of tricking people by delivering links to phony websites that seem like drive links, m-banking, wedding invitations, and other similar content. Phishing arises from WhatsApp users' continued ignorance and disregard for the protection of their personal information. The study's findings indicate that phishing has a significant effect on WhatsApp users directly.

Pendahuluan

Seiring dengan pesatnya perkembangan teknologi informasi, penggunaan aplikasi berbasis internet semakin meluas, termasuk di Indonesia. WhatsApp menjadi salah satu aplikasi perpesanan yang paling banyak digunakan, baik untuk komunikasi pribadi maupun bisnis. Kemudahan dan kecepatan dalam mengirim pesan, serta fitur-fitur tambahan seperti panggilan suara dan video, membuat WhatsApp menjadi pilihan utama banyak pengguna. Namun, popularitas dan aksesibilitas WhatsApp juga menarik perhatian para pelaku kejahatan siber yang melihatnya sebagai ladang subur untuk melakukan serangan phising melalui aplikasi WhatsApp. Phising merupakan salah satu ancaman keamanan siber yang paling umum dan efektif digunakan oleh penjahat siber untuk mencuri informasi pribadi dan sensitif dari korbannya. Dalam konteks ini, WhatsApp, sebagai salah satu platform komunikasi paling populer di dunia, telah menjadi target utama bagi serangan phising.

Modus operandi phising melalui WhatsApp seringkali dimulai dengan pesan teks yang mengandung tautan atau link. Tautan ini biasanya mengarahkan korban ke situs web palsu yang dirancang menyerupai situs resmi dari berbagai layanan atau perusahaan. Situs web palsu ini dibuat sedemikian rupa agar terlihat asli, sehingga korban tidak menyadari bahwa mereka sedang diarahkan untuk memberikan informasi pribadi, seperti data login, nomor kartu kredit, atau informasi keuangan lainnya, kepada penipu.

Salah satu contoh kasus phising yang menonjol di Indonesia adalah kasus penipuan melalui WhatsApp yang terjadi pada tahun 2020. Seorang wanita di Jakarta menerima pesan dari seseorang yang mengaku sebagai perwakilan dari sebuah bank ternama. Pesan tersebut berisi informasi bahwa rekening bank miliknya mengalami masalah keamanan dan diminta untuk mengklik tautan yang disediakan untuk memverifikasi identitasnya dan mengamankan akun.

Tanpa curiga, wanita tersebut mengklik tautan tersebut dan diarahkan ke situs web yang terlihat persis seperti situs resmi bank. Di situs tersebut, dia diminta untuk memasukkan informasi pribadi dan data login rekening bank. Setelah informasi tersebut dimasukkan, penipu segera menggunakan data tersebut untuk mengakses dan menguras dana dari rekening bank korban. Korban baru

menyadari telah menjadi korban phising setelah melihat saldo rekeningnya yang berkurang drastis dan menghubungi pihak bank untuk melaporkan kejadian tersebut.

Data tentang korban phising di Indonesia menunjukkan bahwa insiden semacam ini bukanlah kasus yang terisolasi. Menurut laporan dari Kementerian Komunikasi dan Informatika (Kominfo), jumlah insiden phising di Indonesia meningkat signifikan dalam beberapa tahun terakhir. Pada tahun 2021, terdapat lebih dari 5.000 laporan kasus phising yang diterima oleh Kominfo, meningkat dari sekitar 3.000 kasus pada tahun sebelumnya. Survei yang dilakukan oleh Indonesia Cyber Security Forum juga menunjukkan bahwa hampir 40% pengguna internet di Indonesia pernah menerima pesan phising, dan sekitar 10% dari mereka mengaku pernah menjadi korban. Penelitian tersebut juga menemukan bahwa mayoritas korban phising di Indonesia berusia antara 25 hingga 40 tahun, yang merupakan kelompok usia yang paling aktif menggunakan internet dan aplikasi pesan instan seperti WhatsApp.

Selain itu, laporan dari berbagai bank di Indonesia mengungkapkan bahwa serangan phising sering kali menargetkan nasabah perbankan, dengan modus yang mencakup pengiriman tautan palsu melalui pesan teks atau email yang mengarahkan nasabah ke situs web tiruan. Bank Indonesia dan Otoritas Jasa Keuangan (OJK) telah mengeluarkan peringatan kepada masyarakat untuk lebih berhati-hati dan meningkatkan kewaspadaan terhadap serangan phising, terutama yang dilakukan melalui platform komunikasi populer seperti WhatsApp.

Ancaman phising ini tidak hanya berpotensi merugikan individu dalam hal kehilangan data pribadi dan keuangan, tetapi juga dapat berdampak pada keamanan data perusahaan jika serangan tersebut menargetkan karyawan yang menggunakan WhatsApp untuk keperluan bisnis. Selain kerugian finansial, serangan phising juga dapat merusak reputasi individu atau perusahaan, serta menimbulkan stres dan ketidaknyamanan bagi korban.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis modus phising yang terjadi melalui WhatsApp, termasuk metode yang digunakan oleh penjahat siber dan cara-cara yang dapat dilakukan pengguna untuk melindungi diri dari ancaman ini. Dengan memahami modus operandi phising dan dampak yang diakibatkannya, diharapkan dapat meningkatkan kesadaran dan kewaspadaan pengguna WhatsApp terhadap serangan phising. Selain itu, penelitian ini juga berupaya untuk memberikan rekomendasi praktis yang dapat diterapkan pengguna untuk menghindari jebakan phising, seperti tidak mengklik tautan mencurigakan, memverifikasi keaslian pesan, dan menggunakan sistem keamanan yang kuat seperti VPN dan antivirus. Melalui analisis mendalam tentang phising di WhatsApp, diharapkan dapat memberikan kontribusi signifikan dalam upaya pencegahan dan penanggulangan ancaman keamanan siber, sehingga pengguna WhatsApp dapat lebih terlindungi dari serangan yang merugikan ini.

Landasan Teori

Penelitian mengenai phising dan serangannya melalui aplikasi pesan instan seperti WhatsApp telah menjadi topik yang semakin penting dalam studi keamanan siber. Literatur yang ada menunjukkan bahwa phising merupakan salah satu bentuk kejahatan siber yang paling umum dan efektif digunakan oleh penjahat siber untuk mencuri informasi pribadi dan finansial.

Definisi dan Jenis-Jenis Phising

Phising adalah bentuk kejahatan siber di mana penyerang mencoba untuk memperoleh informasi sensitif seperti nama pengguna, kata sandi, dan rincian kartu kredit dengan menyamar sebagai entitas terpercaya dalam komunikasi elektronik. Istilah "phising" pertama kali digunakan pada tahun 1996 dan berasal dari kata "fishing" (memancing), yang menggambarkan usaha penyerang untuk "memancing" korban agar memberikan informasi pribadi mereka (Jakobsson & Myers, 2006).

Terdapat berbagai jenis phising, termasuk email phising, spear-phising, whaling, dan smishing (phising melalui SMS). Meskipun email phising adalah yang paling umum, phising melalui aplikasi pesan instan seperti WhatsApp (juga dikenal sebagai smishing) semakin meningkat karena tingginya penggunaan aplikasi tersebut di kalangan masyarakat (Hong, 2012).

Penelitian oleh Vishwanath et al. (2011) menunjukkan bahwa platform pesan instan, termasuk WhatsApp, telah menjadi sasaran populer bagi serangan phising karena penggunaannya yang luas dan kemudahan aksesibilitasnya. Serangan phising melalui pesan instan seringkali memanfaatkan kepercayaan antara pengirim dan penerima pesan. Menurut Almomani et al. (2013), pesan phising pada platform ini biasanya mencakup tautan yang mengarahkan pengguna ke situs web palsu yang menyerupai situs resmi, sehingga pengguna tanpa sadar memasukkan informasi pribadi mereka.

Phising melalui aplikasi perpesanan seperti WhatsApp semakin meningkat karena popularitas platform tersebut. WhatsApp, dengan lebih dari dua miliar pengguna aktif bulanan di seluruh dunia (Statista, 2021), menjadi target utama bagi para penjahat siber. Menurut penelitian oleh Kaspersky (2020), serangan phising di aplikasi perpesanan lebih sulit dideteksi karena pesan sering kali datang dari kontak yang dikenal atau melalui grup obrolan, yang menciptakan rasa kepercayaan.

Studi Kasus Phising dan Dampak Serangan Phising

Muftiadi, A., et al. (2019) mengkaji teknik-teknik yang digunakan oleh penjahat siber dalam serangan phising di Indonesia. Penelitian ini mengidentifikasi bahwa teknik social engineering dan penggunaan situs web palsu yang menyerupai situs resmi adalah metode yang paling umum digunakan. Penelitian ini juga menemukan bahwa pesan phising sering kali menciptakan rasa urgensi untuk membuat korban bertindak cepat tanpa berpikir panjang.

Menurut laporan dari Kementerian Komunikasi dan Informatika (Kominfo, 2021), jumlah kasus phising di Indonesia meningkat secara signifikan dalam beberapa tahun terakhir. Survei oleh Indonesia Cyber Security Forum mengungkapkan bahwa hampir 40% pengguna internet di Indonesia pernah menerima pesan phising, dengan sekitar 10% dari mereka menjadi korban. Data ini menunjukkan perlunya peningkatan kesadaran dan edukasi tentang phising di kalangan masyarakat Indonesia. Penelitian oleh Susanto et al. (2013) juga menekankan pentingnya kolaborasi antara pemerintah, sektor swasta, dan masyarakat dalam meningkatkan keamanan siber dan mengurangi dampak serangan phising.

Wibisono, A., et al. (2020) studi kasus serangan phising yang terjadi di Indonesia, termasuk metode yang digunakan dan dampaknya terhadap korban. Salah satu kasus yang dibahas adalah serangan phising terhadap nasabah bank melalui pesan WhatsApp yang mengarahkan korban ke situs web palsu. Adiputra, S., et al. (2021) membahas dampak dari serangan phising terhadap individu dan organisasi di Indonesia. Studi ini menunjukkan bahwa selain kerugian finansial, korban serangan phising juga mengalami stres dan kecemasan yang signifikan. Penelitian ini menekankan pentingnya dukungan psikologis bagi korban selain langkah-langkah teknis untuk mencegah serangan.

Pencegahan dan Perlindungan

Santoso, R., et al. (2020) Menurut Sharma dan Trivedi (2020), ada beberapa langkah yang dapat diambil untuk mencegah serangan phising, termasuk tidak mengklik tautan mencurigakan, memverifikasi keaslian pesan, dan menggunakan perangkat lunak keamanan yang kuat seperti antivirus dan VPN. Selain itu, edukasi dan peningkatan kesadaran pengguna tentang ancaman phising sangat penting. Studi oleh Srikwan dan Jakobsson (2010) menunjukkan bahwa pengguna yang teredukasi lebih mampu mengenali tanda-tanda phising dan lebih kecil kemungkinannya menjadi korban.

Tinjauan Kebijakan Pemerintah dan Peran Edukasi dalam Pencegahan Phising

Kurniawan, T., et al. (2021) dalam "Jurnal Kebijakan Keamanan Siber" mengevaluasi kebijakan pemerintah Indonesia dalam melawan serangan phising. Penelitian ini mengkaji peran Kominfo dan OJK dalam meningkatkan kesadaran publik dan menyediakan alat serta informasi untuk mencegah serangan phising. Studi ini juga mengidentifikasi area yang perlu diperbaiki, termasuk peningkatan kerjasama antara sektor publik dan swasta dalam melawan ancaman siber.

Yuliana, D., et al. (2020) dalam "Jurnal Pendidikan dan Teknologi Informasi" menyoroti pentingnya pendidikan dan pelatihan dalam meningkatkan kesadaran pengguna tentang serangan phising. Penelitian ini mengusulkan program edukasi yang terstruktur dan berkelanjutan untuk membekali pengguna dengan pengetahuan dan keterampilan yang diperlukan untuk mengidentifikasi dan menghindari jebakan phising.

Dari berbagai penelitian yang dilakukan bahwa serangan phising merupakan ancaman serius yang terus berkembang dengan teknik-teknik yang semakin canggih. Modus operandi yang umum melibatkan social engineering dan situs web palsu yang sangat mirip dengan situs resmi. Dampak dari serangan ini tidak hanya bersifat finansial tetapi juga emosional bagi korban. Untuk melindungi diri, pengguna disarankan untuk tidak mengklik tautan mencurigakan, memverifikasi keaslian pesan, dan menggunakan teknologi keamanan seperti VPN dan antivirus. Pendidikan dan peningkatan kesadaran pengguna juga sangat penting dalam pencegahan serangan phising. Kolaborasi antara pemerintah, perusahaan teknologi, dan masyarakat umum diperlukan untuk menghadapi ancaman ini secara efektif.

Metode Penelitian

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan literature review dari sumber-sumber terdahulu. Metode penelitian kualitatif, menurut Muftiadi et al., adalah penelitian yang berfokus pada aspek-aspek penting dalam suatu ruang lingkup atau objek penelitian. Dalam konteks ini, metode deskriptif dipilih untuk mendeskripsikan fenomena serangan phising terhadap pengguna WhatsApp secara mendalam dan komprehensif.

Pendekatan literature review merupakan teknik yang digunakan untuk membaca dan menganalisis data yang bersumber dari berbagai referensi, seperti makalah ilmiah, buku, artikel, dan publikasi lainnya. Literature review memungkinkan peneliti untuk mengumpulkan informasi yang relevan dan aktual mengenai topik yang sedang diteliti, dalam hal ini serangan phising melalui WhatsApp. Dengan metode ini, peneliti dapat memperoleh gambaran yang lebih luas dan mendetail mengenai modus operandi, dampak, serta strategi pencegahan terhadap serangan phising.

Menurut Adiputra et al. (2021), penelitian deskriptif adalah penelitian yang bertujuan untuk mendeskripsikan fenomena yang ada, baik fenomena alam maupun fenomena buatan manusia. Penelitian deskriptif juga digunakan untuk menganalisis dan mendeskripsikan hasil dari subjek penelitian tanpa memberikan implikasi yang lebih luas. Dalam penelitian ini, pendekatan deskriptif digunakan untuk menggambarkan secara rinci bagaimana serangan phising dilakukan melalui WhatsApp, dampaknya terhadap korban, serta langkah-langkah yang dapat diambil untuk menghindarinya.

Metode deskriptif kualitatif dengan literature review dipilih karena dapat memberikan gambaran yang jelas dan rinci mengenai topik yang sedang diteliti. Dengan mengumpulkan dan menganalisis berbagai sumber literatur, peneliti dapat menyusun narasi yang informatif dan mudah dipahami oleh pembaca. Literature review juga memungkinkan peneliti untuk mengevaluasi berbagai perspektif dan temuan dari penelitian sebelumnya, sehingga dapat memberikan wawasan yang lebih komprehensif dan mendalam mengenai serangan phising di WhatsApp.

Dalam prosesnya, peneliti mengidentifikasi sumber-sumber literatur yang relevan, kemudian membaca dan menganalisis isi dari setiap sumber tersebut. Data yang diperoleh dari literatur kemudian disintesis dan disusun secara sistematis untuk menggambarkan fenomena serangan phising, modus operandi yang digunakan, serta langkah-langkah pencegahan yang efektif. Dengan demikian, penelitian ini dapat memberikan kontribusi yang signifikan dalam memahami dan mengatasi ancaman phising melalui WhatsApp.

Hasil dan Pembahasan

Phising berasal dari bahasa inggris, yaitu “fishing” yang berarti memancing. Strategi phising 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, seperti surat undangan pernikahan, email dari sebuah bank atau perusahaan, link drive, dan sejenis lainnya. Sehingga penipu tersebut dapat mengambil data korban secara tidak sah dan menggunakannya untuk tujuan pribadi.

Modus phising melalui WhatsApp merupakan salah satu bentuk serangan siber yang semakin canggih dan sulit dideteksi oleh pengguna. Penyerang biasanya mengirim pesan teks yang tampak sah, sering kali dengan tampilan profesional atau menyerupai pesan resmi dari layanan atau perusahaan terkenal. Pesan ini biasanya berisi tautan yang mengarahkan korban ke situs web palsu yang dirancang untuk mencuri informasi pribadi, seperti data login, nomor kartu kredit, atau informasi keuangan lainnya.

Salah satu teknik yang sering digunakan dalam modus phising ini adalah teknik social engineering, di mana penyerang memanfaatkan kepercayaan dan ketidaksadaran korban. Misalnya, pesan phising mungkin tampak datang dari kontak yang dikenal korban, seperti teman atau anggota keluarga, atau dari sumber yang terlihat terpercaya, seperti bank atau platform e-commerce. Pesan tersebut sering kali mendesak korban untuk mengambil tindakan segera, seperti mengkonfirmasi akun, memperbarui informasi keamanan, atau mengklaim hadiah.

Situs web palsu yang digunakan dalam serangan phising ini sangat mirip dengan situs resmi, baik dari segi desain, logo, maupun tata letak. Hal ini dilakukan untuk mengelabui korban agar tidak curiga dan dengan mudah memberikan informasi pribadi mereka. Penyerang bahkan bisa menggunakan URL yang mirip dengan URL asli, hanya dengan perbedaan kecil yang sulit dikenali sekilas, seperti penggunaan karakter yang hampir sama atau domain yang sedikit berbeda.

Dampak dari serangan phising melalui WhatsApp bisa sangat merugikan. Korban bisa kehilangan informasi pribadi dan finansial yang penting, yang kemudian bisa digunakan oleh penyerang untuk berbagai aktivitas ilegal, seperti pencurian identitas atau penipuan keuangan. Selain kerugian material, korban juga bisa mengalami stres dan kecemasan akibat serangan tersebut. Dalam beberapa kasus, data yang dicuri bisa digunakan untuk melakukan serangan lebih lanjut atau untuk mengakses akun lain yang dimiliki korban.

Untuk menghindari jebakan phising ini, penting bagi pengguna untuk tidak mengklik tautan yang mencurigakan dan selalu memverifikasi keaslian pesan sebelum mengambil tindakan apapun. Langkah-langkah tambahan yang dapat diambil termasuk menggunakan sistem keamanan yang kuat, seperti VPN dan antivirus, serta meningkatkan kesadaran tentang ancaman phising dan cara mengidentifikasinya. Pengguna juga dianjurkan untuk selalu memperbarui perangkat lunak mereka dan mengaktifkan fitur keamanan tambahan yang tersedia di aplikasi WhatsApp.

Penelitian ini mengungkapkan bahwa serangan phising melalui WhatsApp menjadi semakin marak dan canggih, menargetkan pengguna dengan metode yang semakin sulit diidentifikasi sebagai penipuan. Dari berbagai literatur yang dianalisis, ditemukan bahwa modus operandi phising di WhatsApp seringkali melibatkan pesan teks yang mengandung tautan mencurigakan. Tautan ini biasanya mengarahkan pengguna ke situs web palsu yang dirancang menyerupai situs resmi, dengan tujuan mencuri informasi pribadi seperti data login, nomor kartu kredit, dan informasi keuangan lainnya.

Penelitian ini juga menemukan bahwa situs web palsu yang digunakan dalam serangan phising seringkali memiliki tampilan yang sangat mirip dengan situs asli, termasuk logo, desain, dan bahkan URL yang hampir sama. Hal ini membuat banyak pengguna yang kurang waspada mudah terperangkap dan memberikan informasi pribadi mereka tanpa curiga. Selain itu, penyerang sering kali menggunakan teknik sosial engineering untuk menambah kepercayaan pengguna, seperti mengirim pesan yang tampak berasal dari kontak terpercaya atau menawarkan hadiah menarik. Dampak dari serangan phising ini sangat merugikan bagi korban. Tidak hanya kehilangan data pribadi dan finansial, tetapi juga mengalami kerugian emosional dan psikologis. Korban mungkin merasa cemas dan stres setelah menyadari bahwa mereka telah menjadi korban penipuan. Selain

itu, data yang dicuri dapat digunakan untuk melakukan berbagai tindakan kriminal lainnya, seperti pencurian identitas atau penipuan keuangan lebih lanjut.

Untuk menghindari jebakan phising, pengguna WhatsApp disarankan untuk tidak mengklik tautan yang mencurigakan dan selalu memverifikasi keaslian pesan sebelum mengambil tindakan apapun. Langkah-langkah pencegahan lain yang direkomendasikan termasuk menggunakan sistem keamanan yang kuat, seperti VPN dan antivirus, untuk melindungi data pribadi yang tersimpan di perangkat pengguna. Penelitian ini juga menekankan pentingnya edukasi dan peningkatan kesadaran pengguna mengenai ancaman phising dan cara mengidentifikasinya.

Penelitian ini memberikan wawasan mendalam mengenai modus operandi phising di WhatsApp, dampak yang ditimbulkan, dan langkah-langkah pencegahan yang dapat diambil oleh pengguna. Dengan pemahaman yang lebih baik tentang ancaman ini, diharapkan pengguna WhatsApp dapat lebih waspada dan terlindung dari serangan phising yang merugikan. Literature review yang dilakukan juga menunjukkan bahwa peningkatan keamanan siber dan kesadaran pengguna merupakan kunci utama dalam melawan serangan phising yang semakin canggih dan sulit dideteksi.

Mengidentifikasi dan menghindari jebakan phising memerlukan kewaspadaan dan pengetahuan tentang tanda-tanda umum serangan phising. Beberapa langkah yang dapat diambil oleh pengguna untuk melindungi diri dari serangan phising di WhatsApp antara lain:

1. Pengguna harus selalu berhati-hati terhadap pesan yang meminta informasi pribadi atau keuangan. Pesan-pesan yang mendesak pengguna untuk mengambil tindakan segera atau menawarkan hadiah yang terlalu bagus untuk menjadi kenyataan sering kali merupakan tanda-tanda phising. Pesan-pesan ini biasanya menciptakan rasa urgensi yang membuat korban tergesa-gesa untuk bertindak tanpa berpikir panjang.
2. Sebelum mengklik tautan apa pun yang diterima melalui WhatsApp, pengguna harus memeriksa dengan cermat URL yang disertakan. URL yang mencurigakan sering kali memiliki kesalahan ejaan atau menggunakan domain yang tidak biasa. Mengarahkan kursor ke tautan tanpa mengkliknya dapat membantu pengguna melihat alamat situs sebenarnya. Jika URL tersebut terlihat aneh atau tidak familiar, sebaiknya jangan di klik.
3. Pengguna harus memverifikasi keaslian pesan dengan menghubungi pengirim melalui jalur komunikasi lain yang sah. Misalnya, jika menerima pesan yang tampaknya berasal dari bank, pengguna sebaiknya langsung menghubungi bank melalui nomor telepon resmi atau situs web resmi mereka, bukan melalui tautan yang diberikan dalam pesan.
4. Menggunakan perangkat lunak keamanan yang kuat seperti antivirus dan VPN dapat membantu melindungi data pribadi dari serangan phising. Antivirus yang diperbarui secara teratur dapat mendeteksi dan memblokir situs web phising yang berbahaya. VPN dapat membantu menyembunyikan aktivitas online pengguna dan melindungi data dari pengintai yang tidak diinginkan.
5. Mengaktifkan fitur keamanan tambahan di WhatsApp, seperti verifikasi dua langkah, dapat memberikan lapisan perlindungan ekstra. Verifikasi dua langkah mengharuskan pengguna untuk memasukkan PIN selain kata sandi mereka, membuatnya lebih sulit bagi penyerang untuk mengakses akun.

Selain langkah-langkah ini, edukasi berkelanjutan tentang phising sangat penting. Pengguna harus terus memperbarui pengetahuan mereka tentang teknik-teknik phising terbaru dan tetap waspada terhadap tren serangan siber yang terus berkembang. Mengikuti berita keamanan siber dan mengikuti saran dari pakar keamanan dapat membantu pengguna tetap selangkah lebih maju dari penjahat siber. Penelitian ini menegaskan bahwa kombinasi kewaspadaan, penggunaan alat keamanan yang tepat, dan edukasi yang terus menerus adalah kunci untuk melindungi diri dari jebakan phising di WhatsApp. Dengan memahami tanda-tanda peringatan dan menerapkan langkah-langkah pencegahan yang efektif, pengguna dapat mengurangi risiko terkena serangan phising dan menjaga keamanan data pribadi mereka.

Kesimpulan

Penelitian ini mengungkapkan bahwa 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 dirancang untuk mencuri informasi pribadi dan finansial. Penggunaan teknik social engineering dan tampilan situs web yang menyerupai situs resmi membuat banyak pengguna mudah terjebak dan menjadi korban.

Dampak dari serangan phising ini sangat merugikan, termasuk kehilangan data pribadi dan finansial, serta kerugian emosional dan psikologis bagi korban. Penelitian menunjukkan bahwa insiden phising di Indonesia meningkat signifikan, dengan ribuan kasus dilaporkan setiap tahun. Kelompok usia 25 hingga 40 tahun, yang merupakan pengguna aktif internet dan aplikasi pesan instan, paling rentan terhadap serangan ini. Untuk menghindari jebakan phising, penting bagi pengguna untuk tidak mengklik tautan yang mencurigakan, memverifikasi keaslian pesan yang diterima, dan menggunakan perangkat lunak keamanan yang kuat seperti antivirus dan VPN. Langkah-langkah pencegahan lainnya termasuk mengaktifkan fitur keamanan tambahan di WhatsApp dan terus meningkatkan kesadaran tentang ancaman phising melalui edukasi berkelanjutan.

Kesimpulannya kombinasi kewaspadaan penggunaan alat keamanan yang tepat, dan edukasi yang terus menerus merupakan kunci untuk melindungi diri dari serangan phising di WhatsApp. Dengan pemahaman yang lebih baik tentang modus operandi phising dan penerapan langkah-langkah pencegahan yang efektif, pengguna dapat mengurangi risiko terkena serangan dan menjaga keamanan data pribadi mereka. Upaya kolaboratif antara pemerintah, perusahaan teknologi, dan masyarakat umum sangat diperlukan untuk mengurangi dampak serangan phising dan meningkatkan keamanan siber di Indonesia.

Ucapan Terima Kasih

Puji dan syukur kami panjatkan kepada Allah SWT., karena atas berkat dan rahmat-Nya, kami dapat menyelesaikan karya tulis ilmiah ini. Saya menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, cukup sulit bagi kami untuk menyelesaikan karya tulis ilmiah ini. Terimakasih untuk pihak-pihak yang sudah mendukung dan ikut serta dalam penelitian metode phising terhadap whatsapp terutama untuk dosen pengampu yang memberi dukungan dalam pengerjaan artikel ini. Penulis menyadari dalam penulisan karya tulis ilmiah ini masih terdapat kekurangan, untuk itu diharapkan kritik dan saran yang membangun untuk dapat menyempurnakan karya tulis ilmiah ini. Akhir kata, penulis mengucapkan terima kasih dan semoga karya tulis ilmiah ini dapat bermanfaat bagi semua pihak yang membutuhkan.

Referensi

[1.] Adiputra, S., et al. (2021). Dampak Serangan Phising terhadap Individu dan Organisasi di Indonesia. Jurnal Teknologi Informasi dan Komunikasi.

[2.] A. F. Sutarli and S. Kurniawan, “Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia,” Innov. J. Soc. Sci. Res., vol. 3, no. 2, pp. 4208–4221, 2023, doi: 10.5040/9781635577068-0537.

[3.] Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31.

[4.] G. Lumakto and N. Kumala Dewi, “Mehamami Modus dan Pencegahan Penipuan Penggalanganan Donasi Online,” J. Bimas Islam, vol. 14, no. 2, pp. 393–418, 2021, doi: 10.37302/jbi.v14i2.476.

[5.] Kurniawan, T., et al. (2021). Kebijakan Pemerintah dalam Melawan Serangan Phising. Jurnal Kebijakan Keamanan Siber.

[6.] Lohani, Shivam (2019). Social Engineering: Hacking into Humans. Journal of International

Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1.

[7.] Michael, K., McNamee, A., & Michael, M. G. (2006, June). The emerging ethics of humancentric GPS tracking and monitoring. In 2006 International Conference on Mobile Business (pp. 34-34). IEEE.

[8.] Muftiadi, A., et al. (2019). Teknik Social Engineering dalam Serangan Phising di Indonesia. Jurnal Keamanan Siber Indonesia.

[9.] Rachmawati, D. (2014). Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber. Jurnal SAINTIKOM Vol, 13(3), 210.

[10.] Ramdhani, T., & Nandiyanto, A. B. D. (2021). The use of Whatsapp social media as reinforcement online learning during the COVID-19 pandemic. Indonesian Journal of Multidiciplinary Research, 1(1), 107- 112.

[11.] Ratsameethammawong, P., & Kasemsan, K. (2010). Mobile phone location tracking by the combination of GPS, Wi-Fi and cell location technology. Journal of Communications of the IBIMA. Doi: 10.5171/2010.566928.

[12.] R. Nurdin, E. Ramadhani, P. S. Informatika, F. T. Industri, U. I. Indonesia, and W. Scam, "Investigasi Forensika Digital WhatsApp Scam Dengan Menggunakan Framework D4I," J. Tek. Inform. dan Sist. Inf., vol. 11, no. 1, pp. 158–166, 2024.

[13.] R. P. R. Indra Surya Permana, Carolus Borromeus Krishna Sampurno, "Edukasi Keamanan Digital Menggunakan Aplikasi Getcontact Pada Masyarakat Desa Panongan Lor," Perwira J. Community Dev., vol. 3, no. 2, pp. 42–47, 2023.

[14.] S. Parulian, D. A. Pratiwi, and M. Cahya Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia," Telecommun. Networks, Electron. Comput. Technol., vol. 1, no. 2, pp. 85–92, 2021.

[15.] Santoso, R., et al. (2020). Strategi Pencegahan Serangan Phising. Jurnal Keamanan Informasi Indonesia.

[16.] Sunge, A. S. (2022). Komparasi Machine Learning Memprediksi Phising Dalam Keamanan Website. Prosiding Sains dan Teknologi, 1(1), 135-140.

[17.] Varshney, G., Misra, M., & Atrey, P. K. (2016). A survey and classification of web phishing detection schemes. Security and Communication Networks, 9(18), 6266-6284.

[18.] Wibisono, A., et al. (2020). Studi Kasus Serangan Phising di Indonesia. Jurnal Teknologi dan Keamanan Siber.

[19.] Yuliana, D., et al. (2020). Peran Edukasi dalam Pencegahan Phising. Jurnal Pendidikan dan Teknologi Informasi.