Analisis Modus Penipuan Digital Teknik Phising melalui Aplikasi WhatsApp Menggunakan Metode BPMN (Studi Kasus Pada Peretasan E-Wallet)

Mochamad Nizar Palefi Ma'ady[1], Aisyah Nabila Zahra[2], Muhammad Zidan Darmawan[3], Rosyid Abdillah[4], Purnama Anaking[5]

Program Studi Sistem Informasi, Institut Teknologi Telkom Surabaya, Surabaya
e-mail: nizar@ittelkom-sby.ac.id[1], aisyah.nabila.21@student.is.ittelkom-sby.ac.id[2], muhammad.zidan.21@student.is.ittelkom-sby.ac.id[3], rosyidabdillah@ittelkom-sby.ac.id[4], purnama.anaking@ittelkom-sby.ac.id[5]

Kata Kunci:

Aplikasi Keuangan
Data Pribadi
Malware
Penipuan Digital
Phishing

ABSTRAK

Modus penipuan digital saat ini semakin beragam, hal ini diimbangi dengan kecanggihan teknologi dan meningkatnya jumlah pengguna teknologi. Namun, dibalik kecanggihan teknologi yang ada, banyak ancaman kriminal digital yang harus dihadapi oleh pengguna. Salah satunya adalah penipuan digital. Penipuan digital paling sering terjadi tanpa disadari oleh pengguna adalah *phishing*. *phishing* adalah salah satu teknik penipuan digital untuk mencuri data pribadi penting, seperti kata sandi, nomor kartu kredit, dan informasi lain yang bersifat pribadi. Umumnya penipuan ini disebarkan melalui email palsu yang berasal dari sumber terpercaya seperti bank atau perusahaan. Namun, saat ini juga terdapat modus baru dengan menyebarkan malware melalui file pdf, dan apk yang berisi malware melalui media sosial, seperti whatsapp. Malware ini akan digunakan untuk mencuri data pribadi korban tanpa disadari oleh pemiliknya, seperti kata sandi atau data sensitif lainnya. Dalam penelitian ini analisis difokuskan pada modus penipuan digital menggunakan teknik *phishing* yang menargetkan aplikasi E-Wallet. Pembahasan berupa bagaimana penipu menggunakan teknik *phishing* untuk mencuri data pribadi korban dan bagaimana upaya untuk melindungi diri dari serangan *phishing*. Hasil penelitian nantinya dapat menunjukkan teknik *phishing* seperti apa yang digunakan dan upaya perlindungan diri dari serangan *phishing*.

Keyword:

Financial Application
Personal Data
Malware
Digital Fraud
Phishing

ABSTRACT

The modus operandi of digital fraud is increasingly diverse, which is accompanied by the advancement of technology and the increasing number of technology users. However, behind the sophistication of the existing technology, many digital criminal threats must be faced by users. One of them is digital fraud. The most common digital fraud that occurs without the user's awareness is phishing. Phishing is one of the digital fraud techniques to steal important personal data, such as passwords, credit card numbers, and other important information. Generally, this fraud is spread through fake emails originating from trusted sources such as banks or companies. However, currently there is also new modus by spreading malware through pdf, and apk files that contain malware through social media, such as WhatsApp. This

ISSN: 2598-0076

malware will be used to steal the victim's personal data without the owner's knowledge, such as passwords or other sensitive data. In this research, the analysis will focus on the modus operandi of digital fraud using phishing techniques that target e-wallet applications. The discussion will be how fraudsters use phishing techniques to steal the victim's personal data and how to protect themselves from phishing attacks. The research results will eventually show what phishing techniques are used and how to protect themselves from phishing attacks.

PENDAHULUAN

Era teknologi digital telah mengubah paradigma manusia dalam berinteraksi dan beraktifitas pada berbagai aspek kehidupan. Perubahan ini tentunya memberikan kemudahan bagi manusia untuk beraktifitas, sekaligus memberikan tantangan atau ancaman baru, salah satunya yaitu meningkatnya resiko penipuan digital. Penipuan digital merupakan bentuk kriminalitas yang merugikan pengguna teknologi dengan memanfaatkan berbagai celah, baik melalui kelemahan sistem atau keterbatasan pemahaman manusia, seperti tingkat literasi digital. Menurut Lenny Septiani dalam artikelnya menyatakan, bahwa tingkat literasi digital masyarakat Indonesia setiap tahunnya meningkat sedikit demi sedikit dan sudah masuk dalam kategori sedang dengan skala 1-5. Namun berdasarkan penilaian indeks empat pilar tingkat literasi digital diantaranya, yaitu *digital culture*(budaya dalam media digital), *digital safety* (keamanan digital), *digital skill* (kecakapan digital), dan *digital ethics* (etika dalam menggunakan media digital)[1]. Indeks penilaian keamanan digital memiliki persentase paling kecil dibandingkan tiga pilar lainnya. Dengan rendahnya pilar keamanan digital dapat menjadi indikasi bahwa kesadaran masyarakat akan pentingnya melindungi data pribadi masih rendah.

Salah satu metode penipuan digital dengan memanfaatkan pemahaman literasi digital pengguna adalah *phishing. Phishing* merupakan teknik manipulatif yang mengecoh pengguna untuk mengungkapkan data pribadi korban dengan maksud untuk mengakses data atau mencuri identitas korban[2]. *Phishing* umumnya dikirimkan melalui email yang mengatasnamakan sumber terpercaya, seperti bank atau perusahaan tertentu. Email tersebut akan mengarahkan pengguna untuk mengisi data pribadi atau mengakses tautan yang diarahkan ke situs palsu. Sehingga, penipu dapat mengetahui dan mengakses data pribadi pengguna. Data pribadi adalah data identitas personal seseorang yang bersifat pribadi dan tidak boleh sembarang orang tahu, seperti kata sandi aplikasi, kode OTP, nomor kartu kredit dan data pribadi lainnya yang digunakan secara digital[3].

Namun,semakin luasnya akses internet dan penggunaan media sosial, penipuan *phishing* telah mengalami evolusi signifikan. Penipuan phishing yang umumnya menggunakan media email palsu yang mencoba meniru institusi keuangan tertentu, kini pelaku penyerang dapat memanfaatkan file PDF, dan aplikasi berbahaya (APK) yang terinfeksi malware melalui media sosial, seperti WhatsApp. Malware ini yang menjadi senjata penyerang untuk menerobos sistem atau perangkat korbannya. Malware adalah sebuah *software* atau script berbahaya yang dirancang dengan tujuan

ISSN: 2598-0076

tertentu, seperti mencuri atau merusak data umumnya untuk menguji keamanan suatu sistem[4]. Penyerang dapat menggunakan malware untuk mencuri data pribadi korban, seperti kata sandi atau nomor kartu kredit ketika korban secara tidak sengaja mengaktifkan malware melalui link atau menginstall aplikasi yang terinfeksi malware[4].

Dalam konteks inilah penelitian ini bertujuan untuk menganalisis modus penipuan digital yang menggunakan teknik *phishing* melalui media sosial, salah satunya whatsapp dengan menargetkan aplikasi E-Wallet. E-Wallet merupakan aplikasi dompet digital digunakan untuk melakukan transaksi secara online melalui *smartphone*. Aplikasi ini dapat digunakan untuk melakukan transaksi online, seperti belanja online, pembayaran tagihan, dan transfer uang. Selain itu, E-Wallet merupakan aplikasi yang lebih fleksibel karena selain bisa digunakan untuk transaksi online, e-wallet juga dapat digunakan sebagai opsi metode pembayaran offline dengan menggunakan Qris[3]. Ditambah keamanan dari aplikasi e-wallet relatif rendah karena masih banyak pengguna e-wallet yang kurang memahami bagaimana pengguna bisa menjaga keamanan akun e-wallet-nya di dalam perangkat.

Penelitian ini bertujuan untuk menganalisa modus penipuan digital menggunakan teknik *phishing* dengan target aplikasi e-wallet. Hasil penelitian didalamnya diharapkan dapat memberikan wawasan mendalam tentang penipuan *phishing* yang menargetkan aplikasi e-wallet dan upaya panduan bagi pengguna dalam melindungi diri potensi ancaman tersebut. Dengan memahami dan mengidentifikasikan teknik yang digunakan oleh para pelaku, pengguna diharapkan dapat menambah wawasan dan proaktif dalam menjaga privasi informasi pribadi mereka.

METODE

Penelitian pada artikel ini menggunakan metode penelitian kualitatif. Menurut Muftiadi et al, metode penelitian kualitatif adalah penelitian yang berfokus pada hal penting dalam suatu ruang lingkup atau objek[7]. Sifat yang membedakan penelitian kualitatif dengan penelitian kuantitatif, yaitu bersifat multitafsir sehingga dapat dilihat dari berbagai sudut pandang, berdasarkan fenomena sosial secara menyeluruh, dan dinamis[8]. Sehingga, dapat disimpulkan dengan menggunakan metode penelitian kualitatif penelitian dapat fokus untuk memahami fenomena sosial yang dapat memberikan pandangan mendalam tentang suatu peristiwa agar dapat menjadi pelajaran bagi pembaca.

Jenis penelitian kualitatif yang digunakan yaitu penelitian deskriptif dengan menggunakan metode literature review. Literature review adalah cara menemukan, membaca, dan mengevaluasi literatur penelitian pada bidang yang diminati[9]. Metode ini digunakan untuk mengkaji dan mengkritisi terhadap masalah yang dihadapi dengan menggunakan data sekunder, seperti buku, makalah, artikel, video, dan sumber data lainnya akurat[7]. Oleh karena itu, metode ini digunakan

ISSN: 2598-0076

untuk mengkaji dan menggambarkan tentang fenomena penipuan digital dengan menggunakan teknik *phishing* melalui aplikasi Whatsapp terhadap aplikasi e-wallet.

HASIL DAN PEMBAHASAN

Phishing merupakan kata yang berasal dari bahasa Inggris yaitu ‘fishing’ yang berarti memancing. Teknik *phishing* merupakan teknik yang memancing atau menarik perhatian korbannya untuk mendapatkan data pribadi korbannya. Teknik ini pertama kali dikenal pada 2 Janurari 1996 [10]. Pada umumnya *phishing* dilakukan dengan cara mengirim pesan palsu yang mengatasnamakan suatu institusi atau pihak resmi, seperti email dari bank, perusahaan, atau lamaran kerja untuk mengelabui korbannya agar memberikan data pribadinya. Sehingga, seorang *phisher* dapat memperoleh data korban secara tidak sah dan menggunakannya untuk tujuan pribadi.

Seiring berkembangnya teknologi, teknik *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. Ketika korban *phishing* mengunduh dan membuka file tersebut, maka malware atau virus tersebut akan diinstal ke perangkat korban. Malware ini yang nanti akan bekerja untuk mencuri informasi pribadi korban, seperti nomor kartu kredit atau kata sandi aplikasi e-wallet.

Jenis Bentuk Teknik *Phishing*

Phishing memiliki beberapa bentuk untuk bisa meretas aplikasi e-wallet korbannya, model yang penipuan *phishing* dengan mengirimkan file .pdf atau yang sebenarnya merupakan file .apk untuk mencuri data dan mengambil alih perangkat korban merupakan model *clickjacking*. Model serangan *clickjacking* memiliki beberapa lapisan seperti, aplikasi, foto, atau video untuk menyembunyikan tautan aslinya. Lapisan ini dibuat terlihat resmi, agar korban mengira mereka telah mengklik tombol sebenarnya[11].

Penipuan ini sudah memiliki beberapa modus, diantara yaitu pesan palsu dari kurir paket yang melampirkan foto paket, link tagihan asuransi kesehatan, dan undangan pernikahan yang dilampirkan dengan nama .pdf. Selain itu, setelah mengirim pesan informasi, pelaku akan mencoba untuk meyakinkan korban agar membuka file tersebut dan nantinya akan muncul notifikasi izin aplikasi. Notifikasi tentang perizinan aplikasi ini sangat penting, namun banyak pengguna yang kurang menyadari dampak yang terjadi jika mereka memberikan izin sembarangan terhadap suatu aplikasi yang tidak diketahui fungsinya.

ISSN: 2598-0076

Cara Kerja Teknik *Phishing*

Bentuk *phishing* dengan model *clickjacking* memanfaatkan file apk yang dikirimkan melalui suatu media sosial seperti Whatsapp untuk meretas dan mengambil alih akun atau perangkat korbannya. Selain itu untuk meyakinkan korban, pelaku *phisher* akan menarik perhatian korban dengan mengirimkan modus tertentu, seperti pesan palsu dari kurir dengan melampirkan foto paket. Sehingga, korban akan mengunduh dan membuka file tersebut yang ternyata berisi file .apk. File ini akan diinstal ke perangkat korban dan nantinya akan menampilkan notifikasi izin aplikasi. Notifikasi ini penting namun sering diabaikan oleh korban sehingga mereka dengan asal memberikan izin tanpa mengetahui dampak yang akan terjadi.

Berdasarkan informasi dari Badan Siber Dan Sandi Negara (BSSN), file .apk yang digunakan oleh penyerang dalam modus penipuan ini, tergolong berbahaya karena meminta akses untuk melakukan aktivitas yang mengurangi privasi dari perangkat yang dimiliki oleh korbannya, aktivitas tersebut[12],[13]:

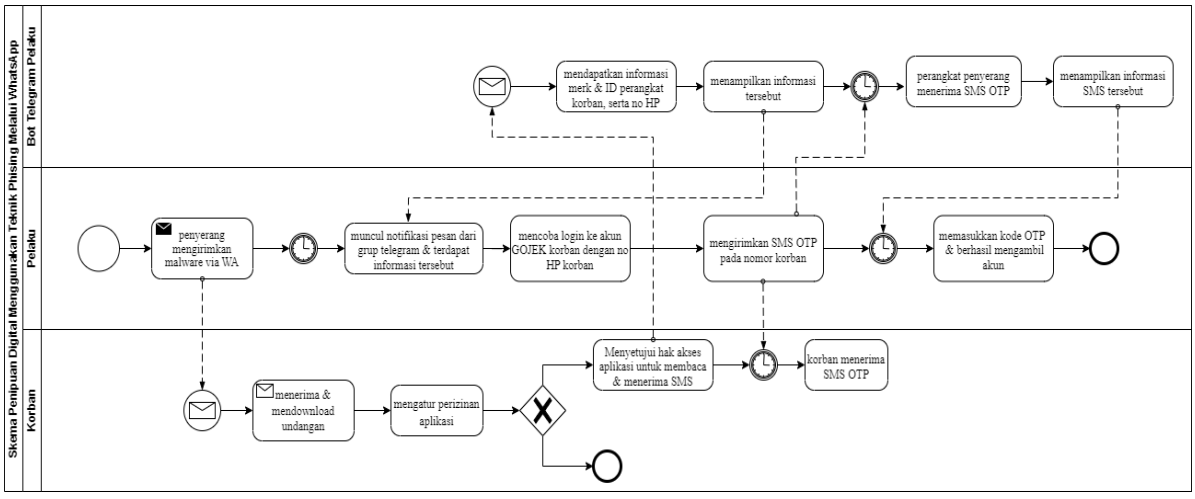
1. Membaca SMS atau MMS

   Jika aktivitas ini diizinkan maka, aplikasi dapat membaca dan memonitor pesan SMS yang diterima di HP atau kartu SIM korbannya. Hal ini juga memberikan akses kepada aplikasi untuk dapat membaca pesan rahasia milik korban seperti transaksi m-banking, otp, dan informasi rahasia lainnya.
2. Menerima SMS dari perangkat korban

   Jika aktivitas ini diizinkan, maka aplikasi dapat menerima semua pesan SMS yang masuk ke perangkat, serta melakukan monitor dan menghapus pesan pada perangkat korban sebelum pemiliknya melihat.
3. Mengirim SMS

   Aktivitas ini, berarti memberikan izin kepada aplikasi agar mampu mengirim SMS yang akan dikenai biaya pengiriman pesan tanpa melakukan konfirmasi pada korban.

Berikut alur peretasan File .apk terhadap Aplikasi E-Wallet menggunakan BPMN:



Gambar 1. BPMN Teknik *Phishing* via media sosial

ISSN: 2598-0076

Berdasarkan alur gambar 1, teknik *phishing* melalui media sosial dengan target aplikasinya yaitu Gojek. Penyerang dapat mengakses mengambil alih perangkat korban ketika aplikasi sudah terinstal dan korban memberikan izin untuk aplikasi melakukan aktivitas yang diminta. Jika semua aktivitas yang diminta itu diizinkan maka dengan aplikasi meminta request data atau dapat menggunakan url Rest API dan akan mengirimkan semua aktivitas perangkat korban ke sebuah bot telegram yang atau perangkat tertentu yang dimiliki oleh pengembang aplikasi. Sehingga, pengembang aplikasi dapat menerima informasi semua aktivitas korban seperti, pesan kode otp, atau transaksi yang dilakukan oleh korban.

SIMPULAN

Phishing merupakan teknik penipuan digital dengan cara mengelabui korbannya menggunakan email atau situs palsu yang mengatasnamakan institusi resmi. Perkembangan zaman, membuat model penipuan teknik *phishing* semakin beragam. Salah satunya yaitu dengan model *clickjacking*. Teknik ini memanfaatkan file .apk untuk mengumpulkan elemen yang digunakan untuk memasang aplikasi android. Aplikasi ini meminta akses mencurigakan yang dapat mempengaruhi privasi pengguna, seperti membaca SMS atau MMS, menerima SMS, dan mengirim SMS. Aplikasi akan meminta request data dan mengirimkan data ke sebuah server. Server yang dikirimkan akan mengirimkan data ke pelaku *phishing*. Sehingga, pelaku dapat menerima segala informasi atau aktivitas korban ketika menggunakan perangkatnya.

DAFTAR RUJUKAN

[1] L. Septiani, “Literasi Digital RI Naik Tipis, tapi Penipuan Online Masih Jadi PR - Teknologi Katadata.co.id,” Feb. 01, 2023. https://katadata.co.id/desysetyowati/digital/63d9e1e820913/literasi-digital-ri-naik-tipis-tapi-penipuan-online-masih-jadi-pr (accessed Aug. 27, 2023).

[2] K. Caniago and T. Sutabri, “Tindak Kejahatan Phising Di Sektor Pelayan Di Universitas Bina Insan Lubuklinggau,” *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)*, vol. 8, no. 1, Art. no. 1, Feb. 2023, doi: 10.30645/jurasik.v8i1.548.

[3] M. B. Yel and M. K. M. Nasution, “KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL,” *Jurnal Informatika Kaputama (JIK)*, vol. 6, no. 1, Art. no. 1, Jan. 2022, doi: 10.59697/jik.v6i1.144.

[4] R. Adenansi and L. A. Novarina, “Malware dynamic,” *JoEICT (Journal of Education And ICT)*, vol. 1, no. 1, Art. no. 1, Mar. 2017, doi: 10.29100/.v1i1.91.

[5] R. Tambunan, “Apa itu E-Wallet? Definisi, Manfaat, dan Cara Menggunakannya.” https://flip.id/blog/apa-itu-e-wallet-dan-cara-penggunaannya (accessed Aug. 26, 2023).

[6] C. O. Winda and Andy, “Pengaruh Sistem Aplikasi E-Wallet, Kualitas Produk, dan Lokasi

ISSN: 2598-0076

terhadap Keputusan Pembelian pada KFC Citra Raya," *EMaBi: Ekonomi Dan Manajemen Bisnis*, vol. 1, no. 3, Art. no. 3, Oct. 2022.

[7] A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking," *Hexatech: Jurnal Ilmiah Teknik*, vol. 1, no. 2, Art. no. 2, Aug. 2022, doi: 10.55904/hexatech.v1i2.346.

[8] A. Fattah, *metode penelitian kualitatif*. CV. Harfa Creative, 2023. Accessed: Aug. 29, 2023. [Online]. Available: http://repository.uinsu.ac.id/19091/1/buku%20metode%20penelitian%20kualitatif.Abdul%20Fattah.pdf

[9] L. Abdillah, "Mengkaji Pustaka (Literature Review)," Mar. 09, 2021. https://deliverypdf.ssrn.com (accessed Aug. 30, 2023).

[10] A. A. Orunsolu, A. S. Sodiya, and A. T. Akinwale, "A predictive model for phishing detection," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 232–247, Feb. 2022, doi: 10.1016/j.jksuci.2019.12.005.

[11] Kompasiana.com, "Cegah Penipuan File .APK, Ini yang Harus Dilakukan WhatsApp," *KOMPASIANA*, Jan. 30, 2023. https://www.kompasiana.com/girilu/63d73df406b56a209e41cb42/cegah-penipuan-file-apk-ini-yang-harus-dilakukan-whatsapp (accessed Sep. 01, 2023).

[12] *Malware Undangan Pernikahan.apk*, (Jun. 10, 2023). Accessed: Sep. 01, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=W98rn22grBs

[13] K. C. Media, "Ramai Penipuan Bermodus File APK, Pahami Cara Kerja dan Tips Menghindarinya Halaman all," *KOMPAS.com*, Feb. 04, 2023. https://money.kompas.com/read/2023/02/05/053000226/ramai-penipuan-bermodus-file-apk-pahami-cara-kerja-dan-tips-menghindarinya (accessed Sep. 01, 2023).

ISSN: 2598-0076