Jurnal Transformasi Bisnis Digital (JUTRABIDI)
Volume. 1 No. 4 Juli 2024
e-ISSN : 3046-8825, dan p-ISSN 3046-8825, Hal. 05-10
DOI: https://doi.org/10.61132/jutrabidi.v1i4.191

Analisis Penipuan Digital Teknik Phishing Terhadap Layanan Mobile Banking

Cut Mutia
Universitas Malikussaleh
Email : cut.220420028@mhs.unimal.ac.id

Rayyan Firdaus
Universitas Malikussaleh
Email : rayyan@unimal.ac.id

Alamat: Jl. Kampus Unimal Bukit Indah, Blang Pulo, Kec. Muara Satu, Kota Lhokseumawe, Aceh 24355
Korespondensi penulis: cut.220420028@mhs.unimal.ac.id

Abstract. *Currently, advances in Internet technology can help the banking sector run its operations better, one of which is the existence of electronic banking (e-banking), and what is popularly used by the public today is Mobile Banking services. It turns out that there are advantages as well as disadvantages, namely the dangers of digital crime. One of the attack techniques that are often carried out to threaten the security of mobile banking is phishing attacks. Phishing is a manipulation technique that tricks users into revealing the victim's data to open the data or steal the victim's identity. The literature review method, which is a method for reading and analyzing data from papers, books, articles, and videos, is used in this kind of research. The research aims to analyze phishing techniques for mobile banking services and find out the types of phishing fraud modes to maintain security in every transaction. The research results can provide information regarding important steps to prevent digital fraud.*

Keywords*: Digital Fraud, Phishing, Mobile Banking Services.*

Abstrak. Saat ini kemajuan teknologi internet dapat membantu sektor perbankan dalam menjalankan operasinya menjadi lebih baik, salah satunya yaitu adanya electronic banking (e-banking) dan yang populer digunakan oleh masyarakat saat ini adalah layanan Mobile Banking. Faktanya, selain kelebihan ada terdapat kekurangan yang dihadapi yaitu adanya ancaman criminal digital. Adapun teknik serangan yang sering dilakukan untuk mengancam keamanan perbankan mobile salah satunya adalah serangan phishing. Phishing merupakan teknik manipulasi yang mengelabui pengguna untuk mengutarakan data pribadi korban dengan maksud untuk membuka data maupun mencuri identitas korban. Jenis penelitian ini menggunakan metode literature riview, yaitu teknik membaca dan menganalisis data yang bersumber dari makalah, buku, artikel, dan video. Penelitian bertujuan untuk melakukan analisis teknik phishing terhadap layanan mobile banking dan mengetahui jenis modus penipuan phishing agar dapat menjaga keamanan dalam setiap transaksi. Hasil penelitian dapat memberikan informasi mengenai langkah penting untuk mencegah penipuan digital.

Kata kunci: Penipuan Digital, Phishing, Layanan Mobile Banking.

LATAR BELAKANG

Teknologi internet yang terus berkembang dengan pesat mengikuti zaman, berdampak positif terhadap berbagai aspek kehidupan masyarakat. Ini membuat orang-orang berfikir bahwa kemajuan teknologi dapat mempermudah proses kegiatan sehari-hari, terutama dalam melakukan transaksi keuangan. Oleh karena itu, layanan yang disediakan melalui internet ini telah memasuki banyak pasar bisnis, khususnya dalam bidang perbankan. Saat ini kemajuan teknologi internet dapat membantu sektor perbankan dalam menjalankan operasinya menjadi lebih baik. Sebagai nasabah, mereka dapat menggunakan internet untuk melakukan banyak

Received: Mei 30, 2024; Accepted: Juni 22, 2024; Published: Juli 30, 2024;
* Cut Mutia , cut.220420028@mhs.unimal.ac.id ---

jenis transaksi keuangan dengan cepat, adanya kemajuan sistem informasi di dunia perbankan, mereka menerbitkan berbagai inovasi salah satunya yaitu adanya electronic banking (e-banking). Contoh electronic banking seperti phone banking mobile banking, SMS banking, automated teller machine (ATM), international electronic fund transfer, dan internet banking. Dari beberapa contoh diatas yang populer digunakan oleh masyarakat saat ini adalah Layanan Mobile Banking (Sari dkk., 2021). Mobile Banking merupakan layanan perbankan yang dapat digunakan dimana saja dalam hitungan jam dan memanfaatkan internet untuk menyampaikan informasi data keuangan dari bank kepada nasabah melalui smartphone, ponsel, dan komputer. Adapun layanan yang diberikan yaitu seperti layanan transaksi, berupa transfer pembayaran tagihan (internet, air, listrik), pembelian pulsa, pembelian tiket, dan informasi (mutasi rekening, saldo, lokasi cabang/ATM terdekat, dan suku bunga). (Rahmahdhani dkk., 2023)

Faktanya, selain kelebihan ada terdapat kekurangan yang dihadapi yaitu adanya ancaman criminal digital dalam bentuk serangan kejahatan siber. Berdasarkan laporan Kaspersky, menjelaskan bahwa di tahun 2023 telah terjadi peningkatan besar terhadap jumlah pengguna mobile banking yang mengalami serangan kejahatan siber, serangan tersebut menargetkan pengguna Android yang meningkat sebesar 32 persen dibandingkan pada tahun 2022. Adapun teknik serangan yang sering dilakukan untuk mengancam keamanan perbankan mobile salah satunya adalah serangan phishing. Pengguna perorangan mengalami proporsi tertinggi kejahatan siber teknik phishing terkait keuangan, yaitu masing-masing sebesar 30,68 persen dan 27,32 persen dari total serangan terhadap pengguna korporat. Phisher menggunakan berbagai metode untuk melakukan aktivitasnya. Misalnya, 41,65% upaya phishing dilakukan menggunakan nama merek terkenal untuk toko elektronik. Phishing merupakan teknik manipulasi yang mengelabui pengguna untuk mengutarakan data pribadi korban dengan maksud untuk membuka data maupun mencuri identitas korban.

Phishing biasanya dikirim melalui email yang mengatasnamakan sumber terpercaya, seperti bank atau perusahaan tertentu. Email tersebut nantinya akan membimbing pengguna agar mengisi data pribadi atau membuka tautan yang diarahkan ke situs palsu. Sehingga, penipu dapat mengetahui serta membuka data pribadi pengguna. Informasi pribadi seperti nomor kartu kredit, password aplikasi, kode OTP yang bersifat pribadi dan tidak boleh diungkapkan kepada orang lain (Palefi Maady dkk., 2023). Penelitian bertujuan untuk melakukan analisis teknik phishing terhadap layanan mobile banking dan mengetahui jenis modus penipuan phishing agar dapat menjaga keamanan dalam setiap transaksi. Hasil penelitian dapat memberikan informasi mengenai langkah penting untuk mencegah penipuan digital.

KAJIAN TEORITIS

Pendapat Vyctoria mengatakan (2013:214) Phishing "Password Harvesting Fishing"adalah modus penipuan yang memanfaatkan pesan palsu dan situs informal yang sepenuhnya bermaksud memperoleh informasi korban sendiri. "Sangat mengkhawatirkan karena trik phishing ini masih banyak digunakan oleh penjahat dunia maya di Asia Tenggara," ujar Yeo Siang Tiong, General Manager Kaspersky untuk Asia Tenggara. Phishing telah menimbulkan banyak korban melalui hiburan online, khususnya di bidang administrasi keuangan. Strategi phishing terkadang dapat mengontrol komputer dan menyebabkan halaman tersebut berubah menjadi halaman pertama, jadi anda harus benar-benar fokus dan juga memastikan bahwa komputer anda tidak terinfeksi untuk menghindari kasus ini karena klien yang menjadi korban mungkin tidak mengerti bahwa mereka telah dirugikan oleh penipuan dari metode phishing ini (Irawan, 2020).

METODE PENELITIAN

Penelitian artikel ini menggunakan teknik deskriptif kualitatif. Sebagaimana dikemukakan oleh (Mulyana, 2008) menggambarkan penelitian sebagai pemeriksaan yang menggunakan teknik logika untuk mengungkap dengan cara menggambarkan informasi dan kenyataan melalui kata-kata secara umum mengenai subjek pemeriksaan. Informasi tersebut dapat diperoleh dari berbagai model, antara lain foto, rekaman video, wawancara, dan temuan studi literatur berdasarkan karya ilmiah (Fiantika dkk., 2022). Jenis penelitian ini menggunakan metode literature riview. Literature riview merupakan teknik membaca dan menganalisis data yang bersumber dari makalah, buku, artikel, dan video. Oleh sebab itu, metode ini digunakan untuk menganalisis peristiwa penipuan digital yang menggunakan teknik phishing dalam cyber crime terhadap layanan mobile banking (Palefi Maady dkk., 2023).

HASIL DAN PEMBAHASAN

1. Cara Kerja Teknik Phishing Dalam layanan Mobile Banking

Phishing berasal dari kata bahasa Inggris "Fishing" yang berarti "memancing", yang bertujuan untuk mengambil dan mendapatkan informasi pribadi korban. Teknik ini digunakan pertama kali pada tanggal 2 Januari 1996. Phishing biasanya dilakukan dengan mengirimkan pesan palsu yang mengatasnamakan organisasi atau pihak resmi melalui email seperti dari perusahaan dan bank, untuk mengelabui korban dan memberikan data pribadinya, sehingga pelaku dapat memperoleh data pribadi korban secara ilegal untuk kepentingan pribadinya. Email tersebut nantinya akan membimbing pengguna agar mengisi data pribadi atau membuka

tautan yang diarahkan ke situs palsu. Sehingga, penipu dapat mengetahui serta membuka data pribadi pengguna. Data pribadi seperti nomor kartu kredit, kata sandi aplikasi, kode OTP, yang bersifat pribadi dan tidak boleh diungkapkan kepada orang lain. Informasi ini kemudian digunakan untuk membuka rekening korban seperti melalui layanan mobie banking untuk memandu nasabah mentransfer sejumlah dana ke rekening tertentu untuk mendapatkan hadiah atau pelaku dapat mengambil habis uang korbannya (Palefi Maady dkk., 2023).

Didalam pelaksanaan teknik phishing sendiri, para pelaku phishing melakukan pemalsuan identitas pribadi yang mengatasnamakan institusi resmi seperti bank. Setelah itu para pelaku akan mengirimkan surat pemberitahuan baik melalui SMS, Email atau yang lebih sering melalui media chat seperti WhatsApp. Disinilah terjadi aksi penipuan digital tersebut biasanya para pelaku kejahatan siber ini akan mengirimkan tautan link yang berisi malware berupa virus, yang digunakan oleh pelaku tersebut serta melakukan aksi penipuan phishing dengan mengumpulkan data pribadi korban (Kurnia dkk., 2022). Selain itu, setelah calon korban membuka tautan berupa link, calon korban akan dikoordinasikan untuk mengisi berbagai informasi individu seperti, tanggal pengakhiran kartu, (PIN) private id number, nomor kartu ATM, kode OTP, (CVV) card konfirmasi nilai, (CVC) cek kartu kode atau kata sandi aplikasi. Ketika calon korban memasukkan informasi individu secara lengkap dan akurat, pelaku pemerasan terkomputerisasi ini dapat mengambil alih kendali atas catatan korban dalam bantuan keuangan portabel ini, dan yang lebih mematikan lagi pelaku melanjutkan aktivitasnya dengan memindahkan aset ke dalamnya dari catatan korban ke catatan pelaku kesalahan penyajian tingkat lanjut (Erdiyanto , 2023).

2. Jenis-Jenis Teknik Phishing Dan Cara Kerjanya

Untuk menghindari penipuan digital seperti teknik phishing ini, perlu diketahui teknik phishing ini memiliki jenis dan cara kerjanya, diantaranya: Phishing Email yaitu dengan mengirimkan email palsu mengatasnamakan bank atau organisasi meminta korban menglkik tautan berupa link untuk mengisi data pribadi pengguna, Spear Phishing yaitu phiser menyelediki tentang korbannya dan mengirimkan pesan resmi kepada korban individu maupun organisasi, Voice Phishing yaitu berupa rekaman suara palsu melalui telpon untuk mendapatkan informasi pribadi korban, SMS phishing adalah phisher mengirimkan pesan melalui SMS sebagai koneksi ke situs palsu, Pharming yaitu pelaku phishing akan memanfaatkan malware untuk mengarahkan korban ke situs palsu, Phishing Media Sosial yaitu menggunakan media sosial untuk mengelabui korbannya melalui Instagram, WhatsApp, Twitter dan Facebook, Phishing melalui aplikasi palsu yaitu pelaku phishing membuat aplikasi ilegal dirancang untuk menipu korbannya (Erdiyanto , 2023).

3. Langkah-langkah Untuk Menghindari Teknik Phishing

Karena penipuan digital semakin parah dan semakin sering terjadi di era teknologi saat ini, penting untuk mengetahui apa yang dapat kita lakukan untuk menghindari teknik penipuan digital seperti phishing pada saat setiap kali menggunakan aplikasi atau mengklik tautan link, diantaranya: Jangan mudah percaya dengan telepon yang mengatasnamakan bank, terutama di luar jam kerja bank, lihat dan periksa kembali nomor telepon biasanya para pelaku phishing menggunakan nomor yang tidak resmi dan mencurigakan, jangan pernah mengikuti perintah email untuk mengklik link yang mencurigakan ke halaman situs web, jangan mengisi data pribadi dari link yang tidak resmi selain situs web resmi dari bank, tidak mudah tergiur oleh hadiah yang diberitahukan oleh seseorang melalui pesan telepon, sms, whatsapp atau email yang harus mentransfer sejumlah uang, jangan memberikan User ID, Password Mobile dan Internet Banking, Pin ATM, atau OTP melalui email, sms, whatapp, atau link web tertentu. (Syah, 2023)

KESIMPULAN DAN SARAN

Dari hasil pembahasan artikel ini dapat disimpulkan bahwa kemajuan teknologi dapat mempermudah proses kegiatan sehari-hari, terutama dalam melakukan transaksi keuangan. Hadirnya layanan mobile banking dapat mempermudah dan mempercepat proses kegiatan transaksi para nasabah. Namun dibalik kelebihan dari kemajuan teknologi terdapat kekurangan yang akan menimbulkan resiko dalam menggunakan layanan mobile banking ini. Salah satunya adanya modus penipuan digital dengan teknik phishing yang semakin banyak memakan korban terutama di era digital saat ini. Untuk menghindari hal ini, kita harus mengetahui berbagai jenis dan pendekatan cara kerja metode phishing dan memahami langkah-langkah apa yang dapat kita ambil untuk menghindari penipuan phishing ini. Dengan mengetahui cara-cara ini, dapat dibayangkan bahwa keamanan informasi anda akan lebih terjaga dan terhindar dari penipuan digital.

Dikarenakan keterbatasan peneliti, Hasil penelitian ini diharapkan dapat dimanfaatkan oleh perbankan sebagai bahan evaluasi dan masukan untuk meningkatkan keamanan layanan mobile banking. Untuk peneliti selanjutnya, terkait dengan modus penipuan digital teknik phishing dapat menambahkan dasar hukum tindak penipuan digital agar dapat mengetahui bagaimana hukuman terkait kejahatan siber dalam melakukan penipuan digital yang dapat merugikan banyak pengguna layanan perbankan mobile.

DAFTAR REFERENSI

Erdiyanto, R. P. (2023). *Jenis dan cara kerja teknik phishing: Penipuan mengatasnamakan bank berbentuk phishing* (p. 75).

Fiantika, dkk. (2022). *Metodologi penelitian kualitatif*. Padang Sumatera Barat: PT. Global Eksekutif Teknologi.

Irawan, D. (2020). *Penipuan digital teknik phishing: Mencuri informasi penting dengan mengambil alih akun Facebook dengan metode phishing* (p. 44).

Kurnia, dkk. (2022). *Penipuan digital di Indonesia*. Universitas Gadjah Mada.

Palefi Maady, dkk. (2023). *Teknik phishing: Analisis modus penipuan digital teknik phishing melalui aplikasi* (pp. 3-4).

Rahmahdhani, dkk. (2023). *Mobile banking: Perlindungan data privasi yang dilakukan perbankan terhadap penggunaan layanan mobile banking* (pp. 88-89).

Sari, dkk. (2021). *Pembayaran digital: Manfaat dan risiko penggunaan layanan perbankan* (pp. 171-172).

Syah, R. (2023). *Langkah menghindari penipuan digital teknik phishing: Strategi kepolisian dalam pencegahan kejahatan phishing melalui media sosial di ruang siber* (pp. 3-4).