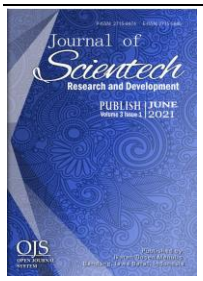

UNES Journal of Scientech Research

Volume 8, Issue 1, June 2023

P-ISSN 2528 5556

E-ISSN 2528 6226

Open Access at: https://ojs.ekasakti.org/index.php/UJSR/

ANALISIS ANCAMAN PHISING TERHADAP LAYANAN ONLINE PERBANKAN (STUDI KASUS PADA BANK BRI)

PHISING THREAT ANALYSIS OF ONLINE BANKING SERVICES (CASE STUDY ON BANK BRI)

Erwin Ginting[1)], Muliada Pardomuan Sinaga[2)], Muhammad Rizal Nurdin[3)], M. Dimas Putra[4)]

[1,2,3,4)] *Program Studi Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Potensi Utama.*

E-mail; erwinginting82@gmail.com, muliadasinaga@gmail.com, mhmmdrizal2911@gmail.com, muhammaddimasputra885@gmail.com

INFO ARTIKEL

Koresponden:

Muliada Pardomuan Sinaga

muliadasinaga@gmail.com

Kata Kunci:

Internet, Legal, Ilegal, Phising, Ancaman Keamanan

Open Access at: https://ojs.ekasakti.org/index.php/UJSR/

Hal : 041 - 047

ABSTRAK

Perkembangan teknologi informasi khususnya internet telah membawa perubahan besar dalam kehidupan sehari-hari, memungkinkan setiap orang melakukan berbagai hal, baik legal maupun ilegal, dengan motivasi untuk meraup keuntungan baik materi maupun immateri. Salah satu ancaman paling umum terhadap keamanan sistem informasi adalah phishing. Phishing adalah metode yang digunakan oleh penjahat dunia maya menggunakan teknik rekayasa sosial untuk menyamar sebagai entitas yang sah dan mencuri informasi pribadi tanpa izin. Ada beberapa faktor yang melatarbelakangi maraknya serangan phishing pada layanan perbankan online. Kurangnya informasi pengguna tentang keamanan data dan kurangnya perlindungan data di media sosial menawarkan peluang bagi penjahat dunia maya untuk mengeksploitasi situasi ini. Untuk mencegah phishing, penting untuk melibatkan jaringan komputer dan menerapkan metode investigasi yang tepat. Salah satu metode yang dapat digunakan adalah pendekatan kualitatif dengan menggunakan teknik deskriptif untuk memahami dan mendeskripsikan fenomena phishing serta mengidentifikasi strategi pencegahan yang efektif. Dengan meningkatkan pengetahuan pengguna, meningkatkan privasi saat menggunakan media sosial, dan menerapkan langkah-langkah keamanan informasi yang ketat di jaringan informasi, diharapkan ancaman phishing dapat dikurangi dan keamanan sistem informasi dapat dipastikan.

Copyright© 2023 UJSR. All rights reserved.

ARTICLE INFO

Koresponden:
Muliada Pardomuan Sinaga
muliadasinaga@gmail.com

Kata Kunci:
Internet, Legal, Illegal, Phishing, Security Threats

Open Access at: https://ojs.ekasakti.org/index.php/UJSR/

Page : 041 - 047

ABSTRACT

The development of information technology, especially the internet, has brought major changes in everyday life, enabling everyone to do various things, both legal and illegal, with the motivation to reap both material and immaterial benefits. One of the most common threats to information system security is phishing. Phishing is a method used by cybercriminals using social engineering techniques to impersonate legitimate entities and steal personal information without permission. There are several factors behind the rise of phishing attacks on online banking services. Lack of user information about data security and lack of data protection in social media offers opportunities for cybercriminals to exploit this situation. To prevent phishing, it is important to engage computer networks and apply proper investigative methods. One method that can be used is a qualitative approach using descriptive techniques to understand and describe the phishing phenomenon and identify effective prevention strategies. By increasing user knowledge, increasing privacy when using social media, and implementing strict information security measures in information networks, it is hoped that phishing threats can be reduced and information system security ensured.

Copyright © 2023 UJSR. All rights reserved.

PENDAHULUAN

Ilmu pengetahuan dan teknologi banyak manfaat pada pekerjaan dan aktivitas sehari-hari masyarakat. Kemajuan teknologi dapat ditandai dengan pertumbuhan ekonomi,mobalitas sosial, perluasan budaya.Perkembangan teknologi dan informasi sangat banyak perkembangan pada beberapa sektor industry dan perbankan, dikarenakan perkembangan teknologi yang pesat sehingga mendapatkan dampak positif seperti efektivitas dan efisiensi waktu, namun dibalik itu terdapat juga dampak negatifnya seperti semakin maraknya cybercrime yang memanfaatkan kelemahan sistem keamanan. Phishing merupakan suatu aktivitas kriminal yang ingin mendapatkan sesuatu informasi dengan menggunakan teknik rekayasa sosial. Pada tahun awal tahun 2022 kasus phising sudah tejadi sebanyak 3.180 kasus yang 50 % dari kasus tersebut adalah lembaga keuangan. Lembaga keuangan adalah salah satu target eksploitasi utama bagi para pelaku cybercrime.

Perbankan sebagai layanan keuangan juga sering terkena Phising. Phishing menggunakan web palsu untuk menipu korban sehingga memasukkan username dan password tanpa sepengetahuan korban. Phishing tidak hanya menyerang Indonesia saja. Pada tahun 2013, Serangan Phishing menyebabkan

kerugian finansial sebesar $ 5,9 Milyar (Rp 80,328 Triliun) di dunia berdasarkan laporan EMC (EMC, 2014). Serangan Phishing tidak hanya menimbulkan kerugian finansial saja. Phishing menyebabkan konsekuensi serius terhadap kehilangan data pribadi pengguna, dan kerugian nama merk perusahaan yang tercemar akibat kasus phishing (Symantec Brightmail TM, 2014) Insiden phishing layanan online yang baru terjadi pada perbankan BRI pada tahun 2022 korban mendapat kerugian sebanyak 1,1 miliar. Uang tersebut hilang dikarenakan korban memasuki layanan yang dikirim oleh pelaku yang tidak bertanggung jawab melalui WhatsApp, pihak BRI juga ikut menginvestigasi kasus ini dan mereka menghimbau agar tidak sembarangan memasuki link yang mengatasnamakan BRI.

Phisihing bukan hanya merugikan secara finansial saja tetapi korban bisa saja mengalami kerugian data dan membawa kerugian juga bagi pihak perusahaan karna hilanganya kepercayaaan masyarakat terhadap produknya. Perkembangan ilmu pengetahuan dan teknologi, khsusunya teknologi informasi sudah terbukti banyak memberi dampak positif bagi semua sektor mulai dari pendidikan sampai industri terbantu berkat ilmu teknologi, tetapi di balik dampak positif beberapa orang yang tidak bertanggung jawab banyak mengambil kesempatan untuk mendapatkan keuntungan baik itu secara finansial maupun non finansial, dikarenakan beberapa orang yang tidak bertanggung jawab tersebut, pengguna suatu produk banyak mengalami kerugian baik itu finansial maupun non finansial.

METODE PENELITIAN

Metode Penelitian merupakan cara yang digunakan untuk memecahkan suatu masalah yang diteliti selama penelitian. Dan pada saat peneelitian menggunakan metode kualitatif. Metode kualitatif adalah metode yang menekankan pada analisis yang medalam, pada suatu objek atau peristiwa yang dapat dijadikan pelajaran untuk mengembangkan ilmu teoritis.

Metode penelitian kualitatif pada artikel ini menggunakan penelitian deskriptif dengan menggunakan metode penelitian kepustakaan. Penelitian akan menggunakan sumber data dari makalah, dan hasil penelitiannya. Oleh karena itu artikel tentang keamanan sistem informasi analisis ancaman di perbankan online akan di pelajari

HASIL DAN PEMBAHASAN

Phising pertama kali ditemukan pada tahun 1996. Menurut James (2005) cara pertama yang dilakukan phisher adalah dengan menggunakan algoritma yang membuat nomor kartu kredit secara acak. Jumlah kredit acak kartu yang digunakan untuk membuat rekening AOL. Akun tersebut kemudian digunakan untuk spam pengguna lain dan untuk berbagai hal lainnya. Programprogram khusus seperti AOHell digunakan untuk menyederhanakan proses. Praktek ini diakhiri oleh AOL pada tahun 1995, ketika perusahaan membuat langkah-langkah keamanan untuk mencegah keberhasilan penggunaan angka kredit secara acak kartu.

Phishing juga dikenal sebegai "Brand Spoofing" atau "Carding", adalah sebuah kejahatan di dunia maya yang merugikan banyak pihak baik itu material maupun non material. Menurut Felten et al (1997), spoofing dapat didefinisikan

sebagai "teknik yang digunakan untuk mendapatkan akses tidak sah ke komputer atau informasi di mana penyerang berkomunikasi dengan pengguna berpura-pura menjadi tuan rumah yang terpercaya."

Faktor penyebab sehingga munculnya ancaman serangan phishing ketika pengguna menggunakan layanan online banking adalah minimnya pengetahuan pengguna, psikologis dan privasi social networking services pengguna. Menurut Dhamija, Tygar, & Hearst (2006) mengungkapkan bahwa pengguna dianggap tidak memiliki pengetahuan yang baik mengenai sistem komputer terutama membedakan domain yang resmi dan palsu.

Cara Kerja Phising

Dari definisi Phising diatas, kita dapat mengetahui bagaimana pekerjaan phishing dilakukan untuk untuk memancing korban kedalam jebakan seorang phisher. Phishing merupakan aktivitas seorang phisher untuk mendapatkan informasi pribadi seseorang pengguna pada saat pengguna menggunakan web palsu yang terlihat seperti tampilan asli atau resmi dari situs web sebenarnya Untuk mengelabui pengguna seorang phisher menggunakan pop-up, email, spanduk agar pengguna terpancing kedalam jebakan seorang phisher agar memberikan informasi pribadi dalam web palsu tersebut. Disisitulah para phisher memanfaatkan kelalaian pengguna untuk mendapatkan informasi pribadinya.

Teknik Phishing

Saat ingin menangkap mangsanya, seorang phiser akan melakukan beberapa teknik seperti:

1. **Internet Submission**

   Internet Submission adalah salah satu metode phishing yang paling canggih. Peretas, juga dikenal sebagai "manusia di tengah", berada di antara situs web sebenarnya dan sistem phishing.

2. **Email spoofing**

   Metode ini biasa digunakan oleh phisher untuk mengirim email kejutaan penggunadengan kedok institusi resmi. Biasanya, email berisi permintaan nomor kredit, kata sandi, atau formulir tertentu untuk diunduh (Joshi, 2012:5)

3. **Manipulasi Tautan (Link)**

   Manipulasi tautan adalah teknik di mana phisher mengirim tautan ke sebuah situs web. Saat pengguna mengklik tautan, itu membuka situs web phishing alih-alih tautansitus web yang sebenarnya

4. **Pesan instan (obrolan)**

   Pesan instan adalah metode di mana pengguna menerima pesan dengan tautan yang mengarahkan mereka ke situs web phishing palsu yang terlihat seperti situs asli.

5. **Host Trojan Host Trojan,**

   Peretas mencoba masuk ke akun pengguna Anda untuk mengumpulkan kredensial melalui komputer lokal Anda. Informasi yang dihasilkan kemudian dikirim Phishing pada layanan internet banking merupakan ancaman dengan menggunakan metode rekayasa sosial untuk menipu pengguna(user). Pengguna tertarik dengan penawaran melalui email,

pesan singkat, telepon dari penjahat yang menyamar sebagai pejabat bank dan mengajak nasabah untuk memberikan data sensitif terkait data pengguna bank (Nasution, 2016). Ada beberapa metode phishing yang bisa di pakai

6. **Rekayasa Sosial**

   Cara ini paling umum digunakan oleh para Phiser karena sangat mudah digunakan untuk mendapat informasi pribadi. Contoh nya seperti" Untuk membantu masyarakat yang terkena bencana alam, Kirimkan data anda sebagai sukarelawan disini"

7. **Manipulasi Link**

   Cara menyesatkan korban dengan cara mengirimkan link lewat email korban, semua isi email sama seperti perusahaan pada umumnya tetapi untuk link mereka membuat sama persis layanan untuk mengambil data korban.

8. **Website Palsu**

   pengguna sebagai korban yang mengunjungi sebuah website phising tidak dapat mengetahui secara pasti apakah website tersebut asli atau palsu karena website tersebut akan dibuat sedemikian rupa sehingga sama dengan aslinya. Contoh kasus seperti itu adalah situs web palsu clickbri.com atau kilkbri.com, yang digunakan untuk menangkap nama pengguna dan kata sandi pengguna yang salah ketik di situs. Sekarang lebih aman karena dilengkapi dengan token untuk menyaring transaksi e-banking.

9. **phising telepon.**

   Model phone phishing digunakan oleh hacker untuk menipu pengguna, biasanya dengan mengirimkan email dengan logo asli bank yang digunakan pengguna. Menggunakan beberapa saran resmi, peretas mengklaim untuk menjaga atau meningkatkan keamanan rekening bank pengguna, pengguna dapat memasukkan kembali nama pengguna dan kata sandi untuk Internet banking atau rekening bank, dan kemudian menambahkan administrator atau layanan dukungan. nomor telepon untuk mengatasi masalah ini. Tetapi semua penyederhanaan ini palsu, dengan harapan pengguna tidak menyadari bahwa dia sedang ditipu dan semua informasi rahasia bahkan mentransfer sejumlah dana ke telepon phishing

10. **Filter evasion**

    seorang ahli phishing/hacker, akan menggunakan teknik ini untuk menghindari jebakan/filter phishing, biasanya menyisipkan gambar untuk phishing agar filter phishing yang dibuat oleh developer tidak dapat mengetahui apakah phishing itu ada atau tidak.

Bank-bank di Indonesia mencegahnya dengan memasang peringatan yang berbunyi: "Waspadalah terhadap trojan, malware, dan spyware. Berhenti! Jika Anda menemukan sesuatu yang tidak biasa selama operasi perbankan Internet, hentikan, jangan lanjutkan!". Namun, semua itu dikembalikan kepada pengguna yang memperhatikan atau mengabaikan pesan tersebut saat menggunakan layanan perbankan online.

Kasus Phising pada BRI

Pada tahun 2022 BRI baru saja terjadi pembobolan di Sumatera Barat, pembobolan diketahui karena korban mendapat informasi melalui Whatsapp tentang perubahaan biaya transfer, dan korban masuk kedalam link yang diberikan pelaku. Setelah itu korban mengisi formulir yang diberikan oleh pelaku dan memberikan username dan password nya

Korban mengalami kerugian sebanyak 1,1 M. korban membuat laporan pada tanggal 31 Mei 2022 dan sekarang kasus ini ditangani oleh direktorat reserse kriminal khusu polda Sumatera Barat.

Dampak Phising pada kasus Bank BRI

Dampak pada korban dalam kejadian ini bocornya data pribadi dan akses login pada web. Untuk phisher tidak mendapatkan keuntungan pada kasus ini dikarenakan akan dikenakan pasal378 KUHP untuk tindak pidana penipuan memperoleh informasi pribadi (phishing) melalui pengiriman email, karena Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tidak diatur secara khusus. tentang phising. Dan untuk pihak bank BRI kurangnya kepercayaan pada pelanggan atau customer.

SIMPULAN

Phishing adalah ancaman yang menggunakan teknik rekayasa sosial yang menipu pengguna dengan menyamar sebagai orang yang berwenang. Phishing menyerang berbagai industri, termasuk industri perbankan yang menjadi target terbesar. Faktor penyebab terjadinya phising pada layanan online banking adalah minimnya pengetahuan pengguna, psikologi dan privasi layanan jejaring sosial. Dengan demikian, pencegahan serangan phishing pada layanan online banking dapat dilakukan melalui edukasi pengguna, pencegahan phishing di level email, penggunaan software anti phishing, penggunaan sistem OTP pada sistem perbankan. Bank-bank di Indonesia mencegahnya dengan memasang peringatan yang berbunyi: “Waspadalah terhadap Trojan, malware, dan spyware. Berhenti! Jika Anda menemukan sesuatu yang tidak biasa selama operasi perbankan Internet, hentikan, jangan lanjutkan!”. Namun, semua itu dikembalikan kepada pengguna yang memperhatikan atau mengabaikan pesan tersebut saat menggunakan layanan perbankan online.

DAFTAR PUSTAKA

Rahardjo, Budi. "Keamanan sistem informasi berbasis internet." *Bandung: PT. Insan Indonesia* (2005). Halim Zuhri. (2017). Memprediksi informasi phishing situs web Angler yang penting menggunakan mesin vektor dukungan (SVM). Akses dari https://media.neliti.com/media/publications/234481-predik-website-pemancing-information-pen-7b738b7f.pdf 28 Mei 2019

Mallisza, D., Adri, J., & Ismanto, H. (2022). THE IMPROVING EFORT OF TECHNICAL DRAWING WITH GIVING AN ASSIGNMENT METHODE (RECITATION) STUDENTS GRADE X TKR 1 SMK STATE 2 PAINAN. INTERNATIONAL CONFERENCE

ON GLOBAL EDUCATION, 434-438. Retrieved from http://114.5.194.187/index.php/ICGE/article/view/124

Yudiana, Y., Elanda, A., & Buana, R. L. Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIKRosma Dengan Menggunakan OWASP Top 10. *CESS (Journal of Computer Engineering, System and Science)*, *6*(2), 37-43.Maxmanro. (2019). Cybercrime: definisi, jenis dan metode kejahatan dunia maya. Akses dari https://www.maxmanroe.com/vid/technology/pengertian-cyber-crime.html

Danyl Mallisza, D. M., Khairul Ummi, K. U., Oktariani, O., Evri Ekadiansyah , E. E., & Dahri Yani Hakim Tanjung, D. Y. H. T. (2022). ENSIKLOPEDIA MATA UANG INDONESIA UNTUK PENDIDIKAN USIA DINI DENGAN MENGGUNAKAN MODEL ADDIE. Journal of Scientech Research and Development, 4(2), 379-388. https://doi.org/10.56670/jsrd.v4i2.96

Mallisza, D. (2016). MULTIMEDIA EDUKASI INTERAKTIF PELAJARAN BIOLOGI.

Rahmawati Dian. (2014).Phising sebagai bentuk ancaman di dunia maya. Akses dari https://prpm.trigunadharma.ac.id/public/fileJurnal/hpG3Jurnal%20Dian%20Rahmawaty2014.pdf 28 Mei 2019

Mallisza, D. (2016). The Management System Of Alumni Departement Informatic And Computer Management Ekasakti University. UNES Journal Of Scientech research, 1(1), 88-101.

Pirsa, N., & Sumijan, S. (2020). Meningkatkan Keamanan Sistem Informasi Puskesmas Terpadu dengan Metode Grey-Box Penetration Test Menggunakan Computer Assisted Audit Techniques. *Jurnal Informasi dan Teknologi*, 133-138.

Azis, H., & Fattah, F. (2019). Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing. *ILKOM Jurnal Ilmiah*, *11*(2), 167-174