HEXATECH
Jurnal Ilmiah Teknik
Vol 1 No 2 Agustus 2022
ISSN: 2828-8696 (Print) ISSN: 2828-8548 (Electronic)
Open Access: https://jurnal.arkainstitute.co.id/index.php/hexatech/index

# Studi kasus keamanan jaringan komputer: analisis ancaman *phising* terhadap layanan *online banking*

**Amin Muftiadi[1], Tri Putri Mulyani Agustina[2], Margaretha Evi[3]**
[1,2,3]Universitas Duta Bangsa Surakarta
[1]190104001@fikom.udb.ac.id , [2]190104020@fikom.udb.ac.id , [3]margaretha@udb.ac.id

**Info Artikel :**
Diterima :
5 Agustus 2022
Disetujui :
15 Agustus 2022
Dipublikasikan :
25 Agustus 2022

**ABSTRAK**

Perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK) khususnya Teknologi Informasi (Information Technology) seperti internet sangat mendukung setiap orang dalam mencapai tujuan hidupnya dalam waktu yang singkat, baik legal maupun ilegal dengan menghalalkan segala cara karena ingin memperoleh materi atau non -manfaat materi. Phishing adalah ancaman yang menggunakan teknik rekayasa sosial yang mengelabui pengguna dengan meniru identitas entitas yang berwenang. Phishing menyerang berbagai sektor industri termasuk industri perbankan yang menjadi target terbesar. Faktor penyebab terjadinya phishing pada layanan online banking adalah minimnya pengetahuan pengguna, psikologi, dan privasi layanan jejaring sosial. Oleh karena itu, pencegahan serangan phising pada Layanan Online Banking dapat dilakukan melalui pengamanan jaringan komputer. Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif dengan teknik deskriptif.

**Kata kunci: Perbankan online, Phishing, Jaringan komputer**

***ABSTRACT***

*The development of Science and Technology (IPTEK), especially Information Technology (Information Technology) such as the internet really supports everyone in achieving their life goals in a short time, both legal and illegal by justifying all means because they want to gain material or non-material benefits. Phishing is a threat that uses social engineering techniques that trick users by impersonating an authorized entity. Phishing attacks various industrial sectors including the banking industry which is the biggest target. Factors causing phishing in online banking services are minimal user knowledge, psychology, and privacy of social networking services. Therefore, prevention of phishing attacks on Online Banking Services can be done through computer network security. The research method used in this study is a qualitative method with descriptive techniques.*

***Keywords : Online banking, Phishing, Computer network***



## PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi (ISTEK), khususnya teknologi informasi (information technology) seperti internet, sangat mendukung setiap orang dalam mencapai tujuan hidupnya dalam waktu yang singkat, baik legal maupun ilegal, menghalalkan segala cara dengan kenyataan bahwa mereka ingin menerima manfaat material atau tidak berwujud. - barang material.Perkembangan teknologi informasi dan komunikasi (TIK) di dunia sangat bermanfaat bagi berbagai sektor industri, perbankan dan usaha kecil dan menengah (UKM). Sektor-sektor ini mendapat manfaat dari efisiensi dan efektivitas dalam hal operasi serta peningkatan pengalaman pengguna. Namun perkembangan ini menimbulkan masalah baru dengan munculnya berbagai cybercrime oleh pihak-pihak yang mencoba memanfaatkan kelemahan sistem dan kesadaran pengguna tentang sistem informasi.

Salah satu bentuk kejahatan dunia maya yang dilakukan oleh scammers adalah phishing. Phishing adalah aktivitas kriminal yang menggunakan teknik rekayasa sosial. Satuan Tugas Anti-Phishing melaporkan bahwa pada kuartal kedua 2014, layanan pembayaran adalah sektor yang paling ditargetkan industri, dengan 39,80% serangan dalam periode tiga bulan dari April hingga Juni 2014,

sementara layanan keuangan terus mengikuti. %. Sektor keuangan menjadi salah satu sasaran eksploitasi para pelaku penipuan. Perbankan sebagai layanan untuk transaksi keuangan massal tidak kebal dari scammers cybercrime. Phishing dapat menggunakan halaman web palsu (menyamar sebagai situs resmi bank) untuk menipu dan mencuri identitas pengguna.

Insiden phishing marak terjadi pada layanan perbankan online di bank-bank di Indonesia. Kepala Otoritas Jasa Keuangan melaporkan, sejak tahun 2013, pengguna merugi Rp 100 miliar akibat kasus pencurian dengan "phishing" (PT. Kompas Cyber Media, 2015). Pada tahun 2015, dua bank besar di Indonesia, yakni Bank BCA dan Bank Mandiri mengimbau penggunanya untuk berhati-hati dalam bertransaksi melalui internet banking. Pengguna diminta untuk mengetahui pesan tentang sinkronisasi token di situs web kedua bank, jika pengguna tidak melakukan transaksi apa pun di layanan "Internet banking". Serangan phishing tidak hanya membawa kerugian finansial. Phishing membawa konsekuensi serius dalam bentuk hilangnya data pribadi pengguna dan hilangnya merek dagang perusahaan, yang dinodai oleh insiden phishing.

Perkembangan ilmu pengetahuan dan teknologi (ISTEK), khususnya teknologi informasi (information technology) seperti internet, sangat mendukung setiap orang dalam mencapai tujuan hidupnya dalam waktu yang singkat, baik legal maupun ilegal, menghalalkan segala cara dengan kenyataan bahwa mereka ingin menerima manfaat material atau tidak berwujud. - barang material. Ini tentu saja merupakan celah dari orang-orang yang tidak bertanggung jawab. Orang-orang ini mencari celah bagaimana mendapatkan materi yang melimpah dengan cara yang sangat singkat. Dengan bantuan Internet, mereka dapat mempelajari hal-hal yang seharusnya tidak mereka praktikkan dalam kehidupan sehari-hari. Karena tentunya merugikan orang lain.

## METODE PENELITIAN

Metode penelitian adalah cara yang digunakan untuk memecahkan masalah yang akan diteliti selama penelitian berlangsung. Saat menulis artikel ini, peneliti menggunakan metode penelitian kualitatif. Penelitian kualitatif adalah penelitian yang menekankan pada kualitas atau hal terpenting dalam sifat suatu barang atau objek. Yang terpenting dalam barang atau jasa berupa peristiwa/fenomena/gejala sosial adalah makna di balik peristiwa tersebut, yang dapat dijadikan pelajaran berharga untuk mengembangkan konsep teoritis.

Oleh karena itu, jenis penelitian kualitatif yang digunakan adalah penelitian deskriptif dengan menggunakan metode penelitian kepustakaan. Kritik sastra merupakan metode penelitian yang dilakukan untuk mengkaji dan mempertimbangkan secara kritis masalah yang diteliti. Peneliti akan menggunakan sumber data sekunder yang diperoleh dari dokumen, arsip, buku, makalah, makalah, dan hasil penelitian lainnya. Dalam metode analisis data, Milles dan Huberman (1984) menyatakan bahwa ada beberapa langkah yang perlu dilakukan peneliti dalam melakukan analisis data, yaitu reduksi data, display data, dan inferensi atau validasi. Oleh karena itu, dalam artikel tentangContoh praktis keamanan jaringan komputer: analisis ancaman phishing di perbankan online untuk mempelajari lebih lanjut masalah yang dihadapi.

## HASIL DAN PEMBAHASAN

Phishing pertama kali diperkenalkan pada tahun 1995. Menurut James (2005), cara pertama yang digunakan phisher adalah menggunakan algoritma yang menghasilkan nomor kartu kredit secara acak. Jumlah kartu kredit acak yang digunakan untuk membuat akun AOL. Akun tersebut kemudian digunakan untuk mengirim spam ke pengguna lain dan untuk tujuan lain. Untuk menyederhanakan proses, program khusus seperti AOHell digunakan. Praktik ini diakhiri oleh AOL pada tahun 1995 ketika perusahaan menerapkan langkah-langkah keamanan untuk mencegah keberhasilan penggunaan nomor kartu kredit acak.

Phishing, juga dikenal sebagai "Brand Spoofing" atau "Carding", adalah bentuk layanan yang menyesatkan Anda dengan mengatakan bahwa data Anda legal dan aman. 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."

Phishing di Internet banking merupakan ancaman dengan menggunakan metode rekayasa sosial untuk menipu pengguna (pelanggan). Pengguna tertarik dengan penawaran melalui email, pesan singkat, panggilan telepon dari penjahat yang menyamar sebagai pejabat bank dan mengajak nasabah

untuk memberikan data rahasia terkait data pengguna bank. Faktor penyebab ancaman serangan phishing ketika pengguna menggunakan layanan perbankan online adalah kurangnya kesadaran pengguna, psikologi dan privasi pengguna layanan jejaring sosial.

**Cara Kerja Phishing**

Dari definisi phishing, Anda dapat melihat bagaimana pekerjaan phishing dilakukan untuk memancing korban ke dalam jebakan phisher. Phishing adalah aktivitas seseorang untuk mendapatkan informasi sensitif pengguna menggunakan email dan situs web palsu yang terlihat seperti tampilan dan nuansa asli atau resmi dari situs web yang sebenarnya.

Phisher menggunakan email, spanduk, atau pop-up untuk mengelabui pengguna agar dialihkan ke halaman web palsu tempat pengguna diminta memberikan informasi pribadi. Di sinilah para phisher memanfaatkan ketidakpedulian dan ketidakpedulian pengguna jaringan palsu untuk mendapatkan informasi.

Berikut ini adalah aspek dari ancaman yang terinfeksi oleh virus phishing:

1. Manipulasi Tautan Beberapa metode phishing menggunakan manipulasi tautan agar terlihat seperti alamat institusi aslinya. Broken URL atau menggunakan subdomain adalah trik umum yang digunakan oleh phisher, seperti contoh URL di bawah ini: www.micosoft.com www.mircosoft.comwww.microsoft.com
2. Filter Evasion Phisher menggunakan gambar (bukan teks) untuk memaksa pengguna mengungkapkan informasi pribadi mereka. Untuk alasan ini, Gmail atau Yahoo menonaktifkan gambar untuk email masuk secara default.
   Untuk membuat email phishing terlihat lebih asli, phisher/penipu memposting:
   a. Tautan yang mengarah ke halaman web yang sah tetapi sebenarnya mengarah ke halaman web phishing.
   b. Atau mungkin munculan yang persis seperti halaman resminya

**Teknik phising**

Saat menjebak mangsanya, fizer menggunakan beberapa teknik, antara lain:

1. Email spoofing Metode ini biasa digunakan oleh phisher untuk mengirim email ke jutaan pengguna dengan kedok institusi resmi. Biasanya, email berisi permintaan nomor kredit, kata sandi, atau formulir tertentu untuk diunduh (Joshi, 2012:5).
2. 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.
3. 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.
4. Host Trojan Host Trojan, peretas mencoba masuk ke akun pengguna Anda untuk mengumpulkan kredensial melalui komputer lokal Anda. Informasi yang dihasilkan kemudian dikirim ke phisher.
5. 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 tautan situs web yang sebenarnya.

Phishing di Internet banking merupakan ancaman dengan menggunakan metode rekayasa sosial untuk menipu pengguna (pelanggan). 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 berbagai metode phishing yang sering digunakan dan menargetkan sistem pengguna.

1. Rekayasa sosial, masyarakat merespon peristiwa penting, cara ini sangat efektif digunakan oleh hacker untuk mengumpulkan informasi penting tanpa upaya yang rumit, seperti mengirimkan header email "Bantu masyarakat Aceh yang terkena tsunami, kirimkan informasi Anda sebagai sukarelawan" ,
2. Manipulasi link, cara ini untuk menyesatkan pengguna dengan mengklik salah satu URL di email sah yang dikirim oleh hacker, semua isi email adalah asli dari perusahaan yang mengirimnya, tetapi ada satu link yang ditolak oleh hacker. . yang akan menuju ke server lain yang sebenarnya bukan server (server ilegal). Informasi pengguna kemudian akan dicegat oleh server palsu.

3. 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.
4. 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 clickbca.com atau kilkbca.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.
5. 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.
6. Metode lain dari phishing telepon adalah memasukkan skrip kecil ke situs web perbankan yang sah. Jika pengguna tidak hati-hati, ia akan jatuh ke dalam jebakan yang akan mengarahkan pengguna ke situs palsu tetapi resmi.

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 Bank BCA**

Pada tahun 2001 terjadi kasus pembobolan internet banking bank BCA oleh mantan mahasiswa ITB Bandung dan pegawai media internet (satunet.com) bernama Steven Haryanto. Anehnya, Steven bukanlah seorang insinyur listrik atau komputer, tetapi seorang insinyur kimia. Ide ini muncul ketika Stephen juga salah mengetik alamat situs web. Dia kemudian membeli domain internet seharga sekitar $20 yang menggunakan nama yang orang salah ketik dan terlihat persis seperti situs internet banking BCA.

Dia kemudian membeli domain internet seharga sekitar $20 yang menggunakan nama yang orang salah ketik dan persis seperti situs internet banking BCA, http://www.klikbca.com, misalnya: wwwklikbca.com, kilkbca. .com, klikbca.com, klikbca.com, klikbac.com. Nasabah Bank tidak akan mengetahui bahwa mereka telah menggunakan situs tersebut karena tampilan yang ditampilkan mirip dengan situs aslinya. Peretas dapat memperoleh ID pengguna dan kata sandi dari pengguna yang masuk ke perangkat lunak, tetapi peretas tidak bermaksud untuk melakukan tindakan kriminal seperti mencuri dana pelanggan, ini murni karena penasaran berapa banyak orang yang tidak mengetahuinya. penggunaan klikbca.com serta pengujian tingkat keamanan situs.

Stephen Haryanto bisa disebut hacker karena dia meretas sistem orang lain yang privasinya dilindungi. Jadi tindakan Steven disebut hacking. Steven dapat digolongkan sebagai tipe hacker yang merupakan gabungan dari white hat hacker dan black hat hacker dimana Steven hanya mencoba untuk mengetahui seberapa aman situs internet banking Bank BCA. Disebut white hat hacker karena tidak mencuri dana nasabah, melainkan hanya mendapatkan user ID dan password nasabah yang dimasukkan di situs internet banking palsu. Namun, tindakan yang dilakukan Steven juga termasuk hacker black hat untuk membuat website palsu dengan diam-diam mendapatkan data milik pihak lain. Steven adalah pemindai, sniffer, dan cracker kata sandi.

**Skenario**

Pelaku mengirimkan situs palsu melalui email dengan teks yang mirip dengan situs aslinya, jika pemilik akun tidak jeli maka korban mengklik situs palsu tersebut sesuai petunjuk pelaku, termasuk mengupdate akunnya, untuk informasi lebih lanjut mengenai data pribadi. dari pemilik akun akan

dibawa ke situs palsu yang mereka klik sebelumnya, sehingga penyerang dapat melakukan apa saja dengan informasi tersebut, termasuk mencuri rekening bank.

**Dampak Phishing bank BCA**

Konsekuensi dari kejadian ini adalah kerugian bagi nasabah dan bank, karena informasi pribadi, termasuk akses login situs web, mungkin tersedia untuk orang lain. Sementara peretas tidak mendapatkan keuntungan materi dari ini, bank akan mengalami kurangnya kepercayaan dari pelanggan. Kasus di atas dapat masuk dalam Pasal 378 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.

## KESIMPULAN

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

Andi Siti Nurbaya Sari, A. N. D. I. (2021). Pengaruh Prinsip Kehati-Hatian Terhadap Ancaman Situs Phishing Pada Nasabah Pengguna Internet Banking (Studi Kasus Pada Bank Syariah di Kota Palopo) (Doctoral dissertation, Institut agama islam Negeri (IAIN Palopo)).

Ardiyasa, I. W. (2021). Analisa Serangan Remote Exploit pada Jaringan Komputer dengan menggunakan Metode Network Forensic. Explore, 11(2), 46-52.

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

Jurnal Ekonomi Bisnis Vol. 7 Tidak. 1 Januari 2016 Halaman 1-14 berjudul "Analisis Ancaman Phishing di Online Banking"

Irawan, M. I., Hediyanto, U. Y. K., & Saedudin, R. R. (2022). Implementasi Keamanan Jaringan Pada Cloudfri Dengan Metode Hardening. eProceedings of Engineering, 9(2).

Jurnal Teknologi Informasi Terapan, Vol. 2, No. 2 (2018) dengan judul "Analisis serangan phishing berbasis web pada layanan e-commerce menggunakan metode proses forensik jaringan."

Maxmanro. (2019). Cybercrime: definisi, jenis dan metode kejahatan dunia maya. Akses dari https://www.maxmanroe.com/vid/technology/pengertian-cyber-crime.html 28 Mei 2019

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

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. Telecommunications, Networks, Electronics, and Computer Technologies (telnect), 1(2), 85-92.

Simangunsong, I. D. (2022). Aspek Perlindungan Hukum Atas Data Pribadi Nasabah Pada Penyelenggaraan Layanan Internet Banking (Studi Kasus Pada PT. Bank Syariah Mandiri Cabang Ulee Kareng).

Ju, A. B., Tng, A., Weley, N. C., & Disemadi, H. S. (2021). Perlindungan Nasabah Dalam Penerapan Electronic Banking Sebagai Bagian Aktifitas Bisnis Perbankan Di Indonesia. Jurnal Perspektif Administrasi Dan Bisnis, 2(1), 27-40.

Naufal Herdanto, R. I. Z. A. L. D. I. (2022). Kebijakan Cyber Security Terhadap Keamanan Negara: Studi Kasus Australia Pada Tahun 2010-2020 (Doctoral dissertation, UPN" Veteran" Yogyakarta).