JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 4, Desember 2023
ISSN 3025-0919 (media online)
Hal 999-999

Analisis Serangan *Phising* dan Strategi Deteksinya

Agung Wijoyo[1*], Adeka Saputra[1], Aditia[1], M. Rio Arya Pratama[1], Rici Rahman[1]

[1]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Tangerang Selatan, Banten, Indonesia

Email: [1*]dosen1671@unpam.ac.id, [2]adekasaputra7@gmail.com, [3]adityastikes@gmail.com, [4]muhammadrioap97@gmail.com, [5]rici008@gmail.com

Abstrak−Dalam era digital yang pesat, teknologi informasi telah memperoleh kehidupan sehari-hari, memfasilitasi konektivitas global melalui internet dan platform daring. Meskipun memberikan akses cepat terhadap informasi, layanan, dan sumber daya, pertumbuhan ini juga membuka pintu bagi serangan siber, termasuk serangan *phising* yang merusak. *Phising* melibatkan penyerang yang menyamar sebagai entitas terpercaya untuk memperoleh informasi pribadi korban, dengan menggunakan pesan atau situs web palsu yang meyakinkan. Keberhasilan serangan ini bergantung pada kemampuan penyerang menciptakan pesan yang sulit dideteksi. Makalah ini secara komprehensif membahas masalah serangan *phising*, menyoroti teknik dan taktik penyerang. Fokusnya juga pada strategi deteksi yang efektif untuk melindungi individu, perusahaan, dan lembaga keamanan siber dari serangan ini. Dengan pemahaman yang lebih baik tentang serangan *phising* dan upaya deteksinya, diharapkan dapat diambil langkah-langkah proaktif dalam melindungi diri dan organisasi dari ancaman siber yang terus berkembang.

Kata Kunci: Keamanan Komputer; *Phising*; Keamanan Data; Risiko Teknologi

Abstract−In the rapid digital age, information technology has acquired everyday life, facilitating global connectivity through the internet and online platforms. While providing quick access to information, services, and resources, this growth also opens the door to cyberattacks, including destructive *phising* attacks. *Phising* involves attackers posing as trusted entities to obtain the victim's personal information, using convincing fake messages or websites. The success of these attacks depends on the attacker's ability to create messages that are difficult to detect. This paper comprehensively addresses the issue of *phising* attacks, highlighting attackers' techniques and tactics. The focus is also on effective detection strategies to protect individuals, companies, and cybersecurity agencies from these attacks. With a better understanding of *phising* attacks and their detection efforts, proactive steps can be taken to protect themselves and organizations from evolving cyber threats.

Keywords: Computer Security; *Phising*; Data Security; Technological Risks

1. PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, teknologi informasi telah merasuk ke berbagai aspek kehidupan kita, mulai dari komunikasi, bisnis, hingga pendidikan. Kehadiran internet dan berbagai platform daring telah membuka pintu menuju konektivitas global yang tak terbatas, memungkinkan akses cepat terhadap informasi, layanan, dan sumber daya yang dahulu sulit diakses. Namun, dengan pertumbuhan ini, kita juga dihadapkan pada ancaman yang semakin serius dalam dunia siber, salah satunya adalah serangan *phising*.

Serangan *phising* merupakan salah satu bentuk serangan siber yang paling merusak dan umum terjadi. Dalam serangan *phising*, penyerang menyamar sebagai entitas yang tepercaya, seperti lembaga keuangan, situs *web e-niaga*, atau bahkan orang-orang terkemuka, dengan tujuan untuk mendapatkan informasi pribadi dan sensitif dari korban. Modus operandi mereka mencakup pengiriman email atau pesan palsu yang terlihat autentik, dengan tujuan merayu korban untuk mengungkapkan kata sandi, nomor kartu kredit, atau data pribadi lainnya.

Keberhasilan serangan *phising* seringkali bergantung pada kemampuan penyerang untuk membuat pesan atau situs web palsu yang sangat meyakinkan sehingga korban tidak menyadari bahwa mereka sedang menjadi target penipuan. Akibatnya, serangan *phising* telah menjadi ancaman serius bagi keamanan data dan privasi pengguna internet, serta merugikan perusahaan dan institusi yang menjadi sasaran.

Dalam menghadapi ancaman ini, pemahaman yang mendalam tentang bagaimana serangan *phising* berlangsung dan strategi deteksi yang efektif sangatlah penting. Serangan *phising* telah berkembang menjadi bentuk yang semakin canggih dan taktik yang lebih licik. Oleh karena itu,

diperlukan penelitian dan analisis yang terus-menerus untuk mengidentifikasi pola serangan baru dan mengembangkan metode deteksi yang lebih canggih.

Makalah ini bertujuan untuk membahas secara komprehensif masalah serangan *phising* dengan fokus pada analisis teknik dan taktik yang digunakan oleh penyerang. Selain itu, makalah ini juga akan menguraikan berbagai strategi deteksi yang dapat digunakan oleh individu, perusahaan, dan lembaga keamanan siber untuk mengidentifikasi serangan *phising* sebelum mereka dapat menyebabkan kerugian. Dengan pemahaman yang lebih baik tentang serangan *phising* dan upaya deteksinya, kita dapat mengambil langkah-langkah proaktif dalam melindungi diri dan organisasi dari ancaman siber ini.

2. METODE

Pada penelitian ini yang mengkhususkan pada analisis serangan *phising* dan strategi deteksinya metode kuantitatif digunakan sebagai pendekatan utama untuk mengumpulkan, menganalisis, dan menginterpretasikan data dalam bentuk angka atau statistik. Dengan menggunakan pengumpulan data kuantitatif, peneliti dapat mengukur berbagai faktor terkait keamanan jaringan, seperti jumlah serangan siber, kerugian finansial yang ditimbulkan, atau tingkat kesadaran pengguna terhadap risiko keamanan. Analisis statistik diaplikasikan untuk mengidentifikasi pola dan tren yang signifikan, seperti peningkatan serangan tertentu selama periode waktu tertentu atau efektivitas dari langkah-langkah keamanan yang telah diimplementasikan. Penggunaan data kuantitatif juga memungkinkan penilaian terhadap kinerja teknologi keamanan, seperti *firewall* atau sistem deteksi ancaman, serta pengukuran efektivitas tindakan pencegahan, seperti pembaruan perangkat lunak dan pelatihan pengguna.

3. ANALISA DAN PEMBAHASAN

3.1 Bentuk Penipuan *Phising*

Bentuk paling umum dari *phising* adalah email *phising*, SMS, panggilan telepon, web *phising*, dan *pop-up* di *website* yang tidak dilindungi. Semuanya akan diberi pesan-pesan yang sangat menarik agar calon korban terbujuk. Bahkan tidak jarang juga pesan tersebut dibuat seolah-olah dikirim oleh bank, lembaga pemerintah, atau perusahaan keuangan seperti *PayPal* dan DANA.

Isinya akan mengajak calon korban untuk melakukan suatu tindakan atau memberikan informasi tertentu. Misalnya, Anda mungkin diminta untuk membuka link atau file, menelepon, atau menginstall dan mengupdate aplikasi tertentu. Para pelaku *phising* akan menggunakan segala cara untuk memancing calon korbannya dan mendapatkan akses ke informasi sensitif yang bisa mereka manfaatkan untuk mendapatkan keuntungan.

3.2 Jenis-jenis *Phising*

Ada beberapa jenis-jenis *phising* yang telah diketahui sebagai berikut:

a. *Scam phising*

Scam phising adalah upaya yang dilakukan para pelaku kejahatan *cyber* untuk mengelabui anda agar memberikan informasi pribadi, seperti nomor rekening bank, *password*, dan nomor kartu kredit. Mereka biasanya akan mengirimkan link atau file yang sudah dimodifikasi atau mengandung *malware*. Informasi yang mereka dapat kemudian digunakan untuk membobol akun Anda, mencuri uang, dan melakukan transaksi. Media yang biasanya dimanfaatkan untuk serangan *scam phising* adalah telepon, email, SMS, atau media sosial.

b. *Blind phising*

Dari semua jenis serangan *phising*, *blind phising* adalah jenis yang paling umum terjadi. Serangan ini dikirim melalui email massal dan tidak menggunakan strategi apa pun. Hanya berbekal "untung-untungan" bahwa akan ada penerima yang jatuh ke dalam perangkap mereka untuk mengikuti tindakan dalam email.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 4, Desember 2023
ISSN 3025-0919 (media online)
Hal 999-999

c. *Spear Phising*

Spear phising diambil dari kata ***'spear'*** yang berarti tombak, layaknya pemancing yang melakukan teknik memancing dengan tombak untuk memilih ikan tertentu. Yap, serangan ini dilakukan terhadap kelompok tertentu, bisa saja pejabat pemerintah, pelanggan perusahaan tertentu, atau bahkan orang tertentu. Serangan spear *phising* biasanya dilakukan untuk membobol dan mengakses database khusus guna mendapatkan informasi penting, file rahasia, atau data-data keuangan.

d. *Clone Phising*

Jenis penipuan ini dilakukan dengan mengkloning website asli untuk mengelabui dan menarik pengguna. Umumnya, web *phising* ini akan meminta calon korban untuk memasukkan informasi sensitif pada kolom yang disediakan. Padahal kolom ini nantinya akan mengirimkan informasi tersebut ke si penjahat. Setelah itu, pengguna akan diarahkan ke halaman asli tanpa menyadari bahwa ia sudah menjadi korban kejahatan *phising*.

e. *Whaling*

Istilah ini berasal dari kata *'whale'* dalam bahasa Inggris yang berarti paus. Benar, masih berhubungan dengan aktivitas memancing, jenis *phising* ini menyasar korban 'besar' atau bukan orang biasa. *Whaling* biasanya menargetkan pegawai eksekutif tingkat tinggi atau tokoh terkenal, seperti direktur perusahaan, dengan maksud untuk mengacaukan instansinya. Serangan ini biasanya dilakukan dengan menyamar sebagai salah satu staf pengadilan atau pengumuman terkait situasi internal perusahaan.

f. *Vishing*

Huruf P diganti dengan huruf V karena serangan vishing dilakukan oleh penjahat menggunakan suara (*voice*) untuk melancarkan serangan dan mencari korban *phising*. Anda pasti sudah sering melihat beberapa video yang berseliweran di media sosial terkait telepon penipuan. Ada yang menimbulkan kepanikan dengan memberikan kabar kerabat yang ditangkap polisi atau kecelakaan, atau bahkan dapat hadiah undian. Ujung-ujungnya korban akan diminta untuk mentransfer sejumlah uang tertentu. Pelaku *phising* yang melakukan vishing terkadang menggunakan nomor telepon yang tidak valid atau VoIP untuk menyembunyikan identitasnya.

g. Pharming

Serangan ini dilakukan dengan DNS spoofing dan menjaring korban dalam skala besar. Jadi, DNS adalah sistem yang menerjemahkan domain menjadi alamat IP, dan setiap kali pengguna mencari website di internet dengan mengetikkan URL (misalnya google.com.br), DNS akan mencari alamat IP yang cocok dengan nama domain tersebut di server.

h. *Smishing*

Smishing adalah sebutan untuk jenis *phising* yang dilakukan melalui SMS. Sama seperti jenis penipuan *phising* lainnya, kalimat-kalimat yang dikirim dalam SMS umumnya mendorong penerimanya untuk melakukan sesuatu. Serangan ini juga termasuk yang paling sering terjadi di Indonesia, yang isinya mendesak korban untuk membayar sesuatu, meyakinkan bahwa korban menang lotre, hadiah undian, atau mendapatkan uang dalam jumlah yang fantastis.

3.3 Cara Mengenali *Phising*

Ada beberapa ciri-ciri umum dari *phising*, sebagai berikut:

a. Nominal uang yang terlihat fantastis

Tidak ada hasil yang instan. Kecil sekali peluang seseorang mendapatkan uang dalam jumlah banyak tanpa harus bekerja keras siang dan malam. Jadi, kalau Anda menerima email, telepon, atau chat yang mengatakan bahwa Anda mendapatkan dana hibah atau transfer uang hingga ratusan juta rupiah tanpa alasan apa pun, kemungkinan besar pesan tersebut adalah *phising*.

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 4, Desember 2023
ISSN 3025-0919 (media online)
Hal 999-999

b. Menang undian heboh

Beberapa konten *phising* yang dikirim penyerang akan merayu Anda untuk mengklaim hadiah karena telah berbelanja di platform tertentu, misalnya menang undian tiket jalan-jalan, smartphone, atau mobil. Jangan pernah klik link dalam pesan seperti ini. Pastikan untuk selalu mengecek *platform* tersebut dan pastikan apakah ada promo yang valid, atau hubungi staf dukungan *platform* yang mengaku mengirimkan pesan tersebut untuk mengonfirmasi kebenarannya.

c. Kalimat ajakan terkesan terburu-buru

Kata-kata seperti "Ambil hadiah Anda sekarang atau besok hangus!" bisa menciptakan kesan tersendiri bagi beberapa orang, terutama yang sedang merasa membutuhkan sesuatu. Padahal biasanya platform yang mengadakan undian valid akan menampilkan informasi pemenang di website resmi mereka tanpa desakan untuk segera mengambilnya. Inilah yang dimanfaatkan para penjahat cyber untuk menjebak calon korbannya agar segera mengklik link atau memasukkan data pribadi dan informasi rahasia mereka.

d. Mengancam dengan berita palsu

Rasa panik menjadi salah satu celah psikologi yang sering dimanfaatkan penipu dunia maya. Biasanya mereka melakukannya melalui vishing, menggunakan nada suara yang sedikit menggertak agar Anda bertindak sesuai perintah. Bahkan ada juga sindikat yang menyamar menjadi staf kepolisian, menelepon Anda untuk menyampaikan berita yang menimbulkan rasa panik. Tentu saja setelahnya mereka akan meminta Anda mentransfer sejumlah uang. Jangan langsung gegabah melakukan sesuatu ketika menerima telepon seperti ini. Cobalah hubungi nomor rekan atau kerabat Anda yang mereka sebut mengalami suatu kejadian dan konfirmasikan kebenarannya.

e. Link eksternal

Email atau pesan yang dikirim penjahat sering kali mencantumkan link eksternal palsu yang bisa cukup berbahaya kalau Anda membukanya. Biasanya link tersebut terlihat berasal dari platform email atau media sosial yang mengabarkan bahwa akun Anda terkena hack. Bahkan, tidak jarang para penipu menggunakan domain palsu yang benar-benar mirip aslinya. Untuk memastikan apakah link tersebut valid, coba arahkan mouse ke link tersebut tapi jangan mengkliknya. Lihat URL-nya di pojok kiri bawah browser. Atau, klik kanan URL lalu copy-paste ke notepad untuk melihat tujuannya. Waspada juga terhadap short URL yang sering digunakan untuk menutupi link asli.

f. File berbahaya

Saat menerima email *phising* atau chat dari orang asing yang mencurigakan, waspadai file yang disertakan dalam lampiran pesan. Terkadang penipu pura-pura mengirimkan dokumen seperti bukti transfer, dokumen penting, atau bahkan proposal pekerjaan padahal filenya adalah program executable atau APK yang bisa memicu virus dan pencurian data kalau sampai diinstal.

g. Pengirim tidak dikenal

Kalau tiba-tiba menerima email, telepon, atau chat dari orang tidak dikenal, Anda harus selalu mencurigainya. Hal yang sama berlaku apabila mereka mengaku dari pihak bank, perusahaan besar yang tidak memiliki ikatan dengan Anda, atau orang asing.

3.4 Melindungi Diri dari *Phising*

Agar terhindar dari *phising*, Anda perlu melakukan langkah-langkah keamanan yang mampu menghalau strategi baru para penjahat cyber. Meskipun sudah banyak berita atau banner yang mengingatkan akan bahayanya, Anda bisa melakukan beberapa cara melindungi diri dari *phising* sebagai tindakan preventif.

Langkah-langkah yang bisa dilakukan untuk menghindari *phising* adalah:

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 4, Desember 2023
ISSN 3025-0919 (media online)
Hal 999-999

a. Analisis email dan chat yang diterima

Selalu evaluasi informasi dan maksud pengirim pada email yang Anda terima. Cek bagian header email untuk mengetahui apakah email diterima dari domain yang valid. Untuk chat yang diterima melalui aplikasi WhatsApp atau SMS, selalu pastikan bahwa pengirimnya adalah akun resmi yang biasanya memiliki tanda centang dan langsung nama platform, bukan sekadar nomor telepon.

b. Install software antivirus

Software antivirus berperan cukup krusial mengingat ada banyak sekali jenis ancaman internet selain *phising*. Untuk melindungi diri Anda, gunakan software antivirus terbaik yang ada di pasaran seperti Avast, ESET, Avira atau AVG yang semuanya memiliki versi gratis.

c. Aktifkan verifikasi dua langkah (2FA)

Two factor authentication atau 2FA adalah langkah keamanan tambahan yang mewajibkan dua kali proses autentikasi, dilakukan satu per satu untuk mengecek ulang dan memvalidasi apakah orang yang meminta akses merupakan pengguna yang berwenang. Aktifkan 2FA pada semua akun Anda baik dengan verifikasi SMS atau aplikasi autentikator guna meningkatkan keamanan dan melindungi diri dari *phising*.

d. Gunakan software firewall

Firewall berfungsi sebagai lapisan penghalang yang mengamankan akses Anda di internet. Software ini memeriksa traffic yang masuk untuk mengecek sumbernya serta mencari tahu apakah akses tersebut termasuk dalam blocklist.

e. Install plugin browser anti-*phising*

Anda juga bisa menginstal plugin agar lebih aman setiap kali mengakses website. Tool ini akan mencari tahu apakah ada catatan atau bukti tentang website tersebut dalam daftar blokir. Beberapa plugin anti-*phising* terbaik di antaranya adalah Anti-*Phising* & Authenticity Checker, Netcraft Extension, atau Stop *Phising*.

f. Pasang sertifikat SSL

Selalu pastikan apakah domain yang Anda akses memiliki sertifikat SSL dengan melihat ikon gembok pada kolom alamat browser. Sebab, saat ini SSL adalah teknologi standar yang wajib diterapkan untuk menjamin keamanan transfer data antara server dan website. Kalau ada ikon gembok tersebut, berarti website yang Anda kunjungi kemungkinan aman dari *phising* (Faradilla A, 2022).

4. KESIMPULAN

Kesimpulan dari penelitian ini bahwa phishing merupakan kejahatan digital yang serius, memerlukan pemahaman mendalam tentang pengertian serta teknik yang digunakan oleh penyerang. Teknik tipu daya yang digunakan oleh penjahat digital semakin canggih, dan oleh karena itu, penting untuk memahami cara kerja mereka. Selain itu, identifikasi strategi deteksi yang efektif adalah kunci untuk melindungi diri dan organisasi dari serangan phishing. Kesadaran yang ditingkatkan, implementasi solusi keamanan siber yang kuat, pembaruan rutin, verifikasi identitas, dan pelaporan serangan adalah langkah-langkah penting yang dapat membantu mengurangi risiko serangan phishing. Dengan tindakan pencegahan yang tepat, kita dapat menjaga informasi pribadi dan keamanan siber kita dengan lebih baik dalam era digital yang penuh dengan ancaman ini.

REFERENCES

Agusta Yudi.2007. K-Means – Penerapan, Permasalahan dan Metode Terkait. Jurnal Sistem dan Informatika Vol. 3

JRIIN: Jurnal Riset Informatika dan Inovasi
Volume 1, No. 4, Desember 2023
ISSN 3025-0919 (media online)
Hal 999-999

Arora, P., Deepali, D., dan Varshney, S. 2015. Analysis of K-Means and KMedoids Algorithm For Big Data. International Conference on Information Security & Privacy (ICISP2015), (hal. 507-512). Nagpur,India.

Bates, A. & Kalita, J. 2016. Counting clusters in twitter posts. Proceedings of the 2nd International Conference on Information Technology for Competitive Strategies, pp. 85

Candraditya Pamungkas, W., & Trimuti Saputra, F. (2020). Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling. *Jurnal Riset Komputer)*, *7*(4), 2407–389. https://doi.org/10.30865/jurikom.v7i4.2304

Faradilla A. (2022, December 16). *Apa itu Phising?* 16 Desember 2022.

Hasibuan, A Zaenal .2007. Metodelogi Penelitian Pada Bidang Ilmu Komputer dan Teknologi Informasi. 20 Juli 2018

Musriha, Gilang R. 2014. Pengaruh Intensitas Pemakaian Internet Terhadap Penggunaan Internet untuk Berbelanja Online yang Dimoderasi oleh Consumer Innovativeness Di Surabaya

Nur Jamal Shaid. (2022, November 25). *phising*. 25 November 2022.

Salim, Tomy. 2017. Data Mining Mengidentifikasi Website Phising Menggunakan Algoritma C.45. Jurnal TAM (Technology Acceptance Model) Volume 8

Suryadi Kurniawan. (2020, July 17). *pengertian phising*. 17 Juli 2020.