Formosa Journal of Applied Sciences (FJAS)
Vol. 4, No.3 2025: 831-844

The Dangers of Phishing to Personal Data Security

Budiono[1*], Fachri Rizky Fadillah[2], Novayandra Arinudin[3]
Fakultas Hukum, Universitas Langlangbuana Bandung
Corresponding Author: Budiono budiono28@yahoo.com

A R T I C L E I N F O

Keywords: Phishing, Personal Data Security, Phishing Attacks

Received : 20, January
Revised : 22,February
Accepted: 24, March

A B S T R A C T

Phishing is one type of cybercrime that has a method of manipulating victims, by pretending to be a trusted person or official government service or company then sending a link so that the victim believes and clicks on the link, then sends personal data to hackers and by hackers used to commit other criminal acts. The media used by hackers can be through whatsapp messages, cellphone short messages or through the victim's email. The threat of phishing to personal data security is great, as it can lead to identity theft, financial loss, and misuse of personal information for further crimes. Attackers often utilize a sense of urgency or emotional manipulation to persuade victims to click on a link or open a malicious attachment. Public awareness of the potential dangers of phishing is necessary to keep personal data safe from increasingly sophisticated threats.

DOI prefik: https://doi.org/10.55927/fjas.v4i3.61
ISSN-E: 2962-6447
https://srhformosapublisher.org/index.php/fjas

Bahaya Phising terhadap Keamanan Data Pribadi

Budiono[1*], Fachri Rizky Fadillah[2], Novayandra Arinudin[3]
Fakultas Hukum, Universitas Langlangbuana Bandung
Corresponding Author: Budiono budiono28@yahoo.com

ARTICLEINFO

Kata Kunci: Phishing, Keamanan Data Pribadi, Serangan Phishing

Received : 20, Januari
Revised : 22,Februari
Accepted: 24, Maret

ABSTRACT

Phishing adalah salah satu jenis kejahatan ciber crime yang memiliki metode manipulasi terhadap korban, dengan cara berpura-pura menjadi orang yang terpercaya atau layanan resmi pemerintah atau Perusahaan kemudian mengirimkan link sehingga korban percaya dan meng klik link tersebut, kemudian mengirimkan data-data yang bersifat pribadi kepada hacker dan oleh hacker di pergunakan untuk melakukan tindak pidana lainya. Media yang dipergunakan oleh hacker bisa melalui pesan whatsapp, pesan singkat handphone ataupun melalui email korban. Ancaman phishing terhadap keamanan data pribadi sangat besar, karena dapat menyebabkan pencurian identitas, kerugian finansial, dan penyalahgunaan informasi pribadi untuk kejahatan lebih lanjut. Penyerang sering memanfaatkan rasa urgensi atau manipulasi emosional untuk membujuk korban agar mengklik tautan atau membuka lampiran yang berbahaya. Kesadaran masyarakat tentang potensi bahaya phishing sangat diperlukan guna menjaga keamanan data pribadi dari ancaman yang semakin canggih.

PENDAHULUAN

Kejahatan siber, juga dikenal sebagai cybercrime, adalah berbagai tindakan kriminal yang dilakukan menggunakan komputer, data, dan jaringan internet. Pelaku kejahatan siber biasanya meretas sistem untuk mendapatkan data pribadi korban. Data pribadi tersebut di pergunakan oleh hacker untuk memanipulasi agar mendapatkan keterangan tentang informasi perbankan atau kehidupan pribadi korban agar mendapatkan uang. Salah satu jenis cybercrime yang marak terjadi adalah phising Dimana hacker mencuri data pribadi korban dengan cara mengirimkan link agar korban secara tidak sadar mengirimkan data pribadi kepada hacker tersebut.

Indonesia dengan penduduk terbanyak nomer tiga dunia dengan jumlah kurang lebih 350.000.000 jiwa sebagai pengguna teknologi modern dalam hal ini adalah handpone merupakan sasaran empuk bagi penjahat cyber, dengan demikian sangat penting masyarakat diberikan wawasan dan pengetahuan tentang kejahatan teknologi modern yang sering dikenal sebagai phising. Semakin berkembangnya kemajuan zaman yang berdampak terhadap perkembangan ilmu pengetahuan dan teknologi modern dan akan diikuti berkembangnya kejahatan modern di bidang phising melalui handpone. Kerugian-kerugian akibat kejahatan phising sangat banyak dan yang paling utama adalah kerugian secara ekonomi karena notabenenya kejahatan phising untuk mengambil uang melalui data-data yang dicuri melalui handpone korban, sebagai contoh kasus Seorang korban yang terletak di bali jembrana Bernama I Made Dwi Jana Putra kehilangan uang sejumlah RP. 81 juta rupiah pada bulan oktober tahun 2023 yang lalu, di duga uang korban hilang melalui phising, akibat dari meng klik salah satu link melalui handphonenya. Setelah di cek ulang ternyata ada aplikasi yang terinstal di hancpone korban, tetapi korban tidak merasa menginstal aplikasi tersebut.

Phishing, atau penipuan online, merupakan salah satu jenis tindak pidana cybercrime yang sangat berpotensi berkembang, tetapi penegakan hukum terhadap kasus ini dianggap belum cukup efektif. Kejahatan ini sekarang dilakukan dengan sangat terang-terangan daripada secara sembunyi-sembunyi. Kasus kasus yang ada di Indonesia sering di beritakan di media sosial ataupun media cetak dan elektronik disebarkan melalui keseluruh lapisan Masyarakat dari dewasa hingga anak-anak, yang mana mereka tidak mengikuti perkembangan teknologi modern tentang Bahaya dan tehnik-tehnik phising.

Masalah ini semakin serius karena kurangnya penegakan hukum dan kurangnya kesadaran tentang keamanan siber. Meskipun demikian, kejahatan cyber memiliki potensi besar untuk menimbulkan masalah nasional. Untuk mengatasi hal tersebut terdapat dua cara yang bisa di lakukan oleh pemerintah dan msyarakat yaitu:

1. Meningkatkan minat baca tentang pengetahuan bahaya phising dan informasi yang jelas tentang bahaya phising yang dapat dilakukan oleh pemerintah lewat media cetak atau media elektronik melalui bantuan kepolisian.
2. Peningkatan hukuman dan kejelasan hukum bagi pelaku tindak pidana phising sehingga membuat jera para pelaku phising.

Untuk mencegah ancaman ini, diperlukan pendekatan yang lebih menyeluruh dan berkelanjutan. Kerugian secara ekonomi akibat pengambilan data pribadi korban sering terjadi untuk memeras korban dan jika tidak di turuti korban, maka data pribadi bisa di sebarluaskan, dan jika terjadi di Perusahaan besar dapat mempengaruhi reputasi Perusahaan dan merugikan secara ekonomi akibat hilangnya konsumen di Perusahaan tersebut. Karena dampak-dampak yang sangat bahaya serta minimnya pengetahuan Masyarakat terhadap kejahatan cyber phissing maka perlu sosialisasi dari pemerintah sebagai penyelenggara negara memberikan pengetahuan terhadap warna negaranya. Maka berdasarkan latar belakang diatas yang telah di uraikan penulis, penulis tertarik membuat artikel yang berjudul "Bahaya phising Terhadap Keamanan Data Pribadi".

Identifikasi Masalah

a. Kurangnya pengetahuan masyarakat terhadap kejahatan teknologi modern melalui phising.
b. Upaya untuk mengenali dan memahami bagaimana pelaku phising menipu korban untuk mendapatkan data pribadi.
c. Bagaimana perlindungan hukum untuk konsumen yang menjadi korban phising?
d. Bagaimana dampak-dampak yang ditimbulkan oleh phising?

TINJAUAN PUSTAKA

Phising adalah salah satu cyber crime untuk melakukan penipuan dengan mengelabui korban. Umumnya aksi kejahatan ini dilancarkan melalui email maupun media sosial lain, seperti mengirimi link palsu, membuat website bodong, dan sebagainya. Tujuannya yaitu mencuri data penting korban, seperti identitas diri, password, kode PIN, kode OTP (one time password) pada akun-akun keuangan, seperti mobile banking, internet banking, aplikasi paylater, dompet digital, sampai kartu kredit (Zahro, 2023).

Phising adalah bagian dari kejahatan dunia maya internasional yang dapat mencuri identitas dan uang dan perlidungan konsumen menjadi perhatian utama untuk menghindari kejahatan tersebut (Santoso, 2023). Kata phising berasal dari Bahasa inggris yang artinya memancing, namun dalam Bahasa ciber istilah phising di gunakan untuk memancing korban agar mengklik tautan yang disediakan oleh hacker agar korban tanpa sadar memberikan informasi yang sifatnya pribadi, dan di gunakan oleh hacker untuk kejahatan, ciri khas dari pelaku phising yaitu mereka menyamar menjadi pihak yang berwenang atau teman deket korban supaya dapat dengan mudah memanipulasi korban. Biasanya phising dilakukan pada tahap awal serangan untuk mendapatkan kredensial target (Indrajit, 2016).

Beberapa contoh kredensial target yang menjadi incaran hacker adalah sebagai berikut:

a. Facebook.
b. Bank link.
c. Fax notice.
d. Court secretary complaint.
e. Drobox link.

Jenis Phising

Menurut bakrie.ac.id/articles/599 ada 5 jenis phising yaitu:

1. Phising PDF
   Jenis phising berikut ini adalah jenis yang paling baru muncul belakangan waktu ini. Pencurian data ini disebut-sebut sering melalui pesan WhatsApp yang berkedok file PDF. Ini adalah metode phishing terbaru yang mencoba menyebarkan program aplikasi jahat yang bila dilakukan dapat menyebabkan pencurian data pribadi.
2. Web phising
   Web phishing adalah jenis penipuan dengan cara menyalin website asli untuk menipu dan menarik pengguna. Normalnya situs tersebut akan meminta data-data sensitive korban, kemudian data tersebut dikirimkan ke hacker melalui scamer.
3. Deceptive phising
   Deceptive Phishing adalah jenis penipuan yang mengirimkan email atas nama organisasi yang meminta korban untuk melakukan aktivitas tertentu, seperti: verifikasi informasi akun, berikan nama pengguna, kata sandi, minta korban untuk mengubah kata sandi, lakukan transaksi pembayaran.
4. Blind phising
   Blind phising adalah di mana penipu mengirimkan email atau pesan massal. Fitur utama dari phishing buta adalah scammer tidak menyebutkan nama penerima tertentu karena pesan dikirim ke banyak orang sekaligus.
5. Smishing
   Smishing adalah bentuk phishing yang disebarkan melalui pesan teks (SMS). Jenis phishing ini menjadi salah satu yang paling sering kita temukan. Istilah smishing adalah kombinasi dari SMS dan phishing. Smishing dianggap sangat mudah dilakukan para penipu, mereka hanya perlu merangkai nomor telepon untuk menyebarkan pesan iseng. Contoh penipuan smishing:
   a. Membuat janji palsu
      Penjahat menggunakan berbagai macam taktik penipuan untuk meyakinkan orang agar menyerahkan data pribadi — dan uang. Mereka mungkin memberikan janji palsu: Kartu hadiah, uang hadiah, atau kemenangan lainnya; Kartu kredit berbunga rendah

atau tanpa bunga; Kupon dan diskon lainnya dan Pengampunan utang pinjaman mahasiswa.

b. Menyamar sebagai perusahaan yang sah
   Upaya penipuan juga dapat diduga dilakukan oleh perusahaan sah yang memiliki pertanyaan tentang akun atau transaksi Anda. Mereka mungkin akan Mengaku sebagai perwakilan layanan pelanggan yang perlu memverifikasi informasi akun; Ingin membahas tagihan mencurigakan baru-baru ini atau masalah dengan pembayaran Anda; Kirim faktur palsu dan minta Anda menghubungi mereka jika Anda tidak mengotorisasi pembelian dan Berpura-pura menjadi pemberitahuan atau pelacak pengiriman paket.
c. Memangsa amal
   Penjahat Smishing bahkan dapat memangsa dorongan beramal Anda dengan Meminta sumbangan setelah bencana alam atau peristiwa bencana besar lainnya, seperti bantuan badai atau kebakaran hutan atau Menyamar sebagai orang yang Anda kenal, seperti organisator komunitas atau politisi, yang akan mengumpulkan sumbangan uang.

Dampak-dampak dari Aktivitas *Phising*

Dampak yang terjadi pada korban phising yg paling sering terjadi yaitu: kehilangan akses akun, merusak reputasi Perusahaan, dampak psikologis karyawan, serta kerugian finansial.

METODOLOGI

Pada penelitian ini menggunakan Metode kualitatif dimana metode yang fokus pada pengamatan yang mendalam. Oleh karenanya, penggunaan metode kualitatif dalam penelitian dapat menghasilkan kajian atas suatu fenomena yang lebih komprehensif.

HASIL PENELITIAN DAN PEMBAHASAN

Kejahatan cyber yang terjadi di platform jaringan komputer adalah phising. Phishing adalah tindak pidana yang dilakukan secara online melibatkan penipuan dalam keamanan komputer. (Saputra Gulo dkk., 2020). Tindakan kriminal ini juga mengalami pertumbuhan dan penyebaran yang luas seiring berjalannya waktu. Jaringan komputer juga dapat menjadi sumber ancaman kriminal saat ini. Kemajuan teknologi memberikan banyak manfaat, seperti peluang pekerjaan, partisipasi politik, demokrasi, dan akses informasi. Namun, karena cakupannya yang sangat luas, tindakan kriminal di internet menjadi semakin berbahaya (Alhakim & Sofia, 2021).

Orang yang melakukan kegiatan phising disebut sebagai hacker. Hacker menguasai dan menggunakan bahasa pemrograman komputer. Hacker menyusup atau mengakses jaringan komputer target untuk memahami sistem dan infrastruktur yang digunakan. Untuk mengakses jaringan komputer target, hacker memanfaatkan kelemahan sistem dan dieksploitasi. Dengan kata lain, pencuri memasuki situs web tanpa izin. Bahkan jika situs korban dilindungi oleh sistem keamanan, hacker dengan keahliannya dapat memasuki dan mengendalikan situs tersebut. Hacker memiliki tujuan utama untuk merusak sistem yang digunakan oleh pemilik situs atau aplikasi tertentu. Karena situs atau aplikasi tersebut merupakan properti pribadi milik pemiliknya, hacker yang berhasil memasuki sistem orang lain dianggap sebagai kejahatancybercrime.

Mengubah tampilan atau juga bisa mengubah system situs web secara tidak sah dan menghapus beberapa file di dalamnya adalah merupakan tindakan kriminal karena dapat menyebabkan kerugian bagi pemilik akun. Dalam pandangan kriminologi, ada beberapa faktor dan alasan yang menyebabkan kasus cybercrime phishing terjadi.

Dari segi alasan, kejahatan ini biasanya dapat dikategorikan menjadi dua golongan, yaitu:

a. Motif intelektual kriminal terjadi saat seseorang melakukan kejahatan semata-mata untuk kepuasan pribadi dan untuk menunjukkan kemampuannya dalam merancang dan menerapkan teknologi informasi. Motif ini umumnya dilakukan oleh individu.
b. Motif ekonomi, politik, dan kriminalitas merujuk pada alasan di balik suatu tindak kriminal yang dilakukan dengan tujuan memperoleh keuntungan pribadi atau kelompok yang dapat merugikan pihak lain baik secara ekonomi maupun politis. Kriminalitas dengan motif ini, bertujuan untuk menciptakan dampak besar dan sering kali dilakukan oleh perusahaan atau korporasi.

Faktor utama yang dapat menyebabkan timbulnya kejahatan cyber phishing (Hariyono & Simangunsong, 2023) adalah:

a. Ketidakseimbangan antara kemajuan suatu negara dan kesejahteraan masyarakatnya yang meningkatkan potensi ketimpangan social.
b. Gaya hidup.
c. Kurangnya sosialisasi atau edukasi baik dari lembaga pendidikan seperti sekolah maupun dari orang tua mengenai penggunaan internet yang dapat menyebabkan penyalahgunaan beragam.
d. Peningkatan penggunaan media sosial, media elektronik, dan penyimpanan data virtual (cloud), yang membuat individu semakin terpaku pada akses internet dalam kehidupan sehari-harinya.
e. Kelalaian.
f. Ingin diakui tentang keahliannya oleh orang lain.
g. Kemajuan teknologi dan kemudahan akses internet.

Modus yang paling sering terjadi di Masyarakat melalui handphone adalah korban disuruh transfer uang melalui sms ke nomer rekening tertentu dan di manipulasi agar masuk akal dan menjebak korban.

Awal mula terjadinya kejahatan phishing dapat dipilah menjadi dua faktor, diantaranya:

1. Faktor Teknis, koneksi yang saling terhubung antar jaringan mempermudah pelaku kejahatan dalam melaksanakan tindakannya, sedangkan peningkatan penggunaan teknologi yang tidak merata menyebabkan ketimpangan kekuatan antara pihak-pihak yang terlibat.
2. Faktor Ekonomi, Kejahatan phishing cybercrime bisa dianggap sebagai bagian dari aktivitas ekonomi. Permasalahan yang perlu diperhatikan dalam kejahatan ini adalah keamanan jaringan. Sebagai komoditas ekonomi, cybercrime menjadi bagian dari skenario besar dalam aktivitas ekonomi global.

Terdapat beberapa Upaya yang dapat dilakukan korban saat terdampak phising. Menurut Tim Penelitian dan Analisa Global Kaspersky Laboratorium untuk menghindari dan melindungi diri dari Phishing adalah dengan cara sebagai berikut:

a. Buat bookmark untuk halaman login situs sosial seperti Facebook atau ketik URL www.facebook.com secara langsung di address bar browser Anda.
b. Jangan klik link di pesan email.
c. Hanya ketik data rahasia di website yang aman.
d. Secara teratur periksa akun bank Anda dan laporkan segala sesuatu yang mencurigakan kepada bank Anda.
e. Perhatikan tanda-tanda giveaway dalam email phising: jika itu tidak ditujukan secara pribadi kepada Anda; jika email tersebut diterima oleh lebih dari satu orang; atau jika terdapat kesalahan ejaan, tata bahasa, sintaks, atau kekakuan bahasa lainnya. Ini biasanya dilakukan oleh penyebar phising untuk menghindari filtering.
f. Menginstall software untuk kemanan internet dan tetap mengupdate antivirus.
g. Menginstall patch keamanan.
h. Waspada terhadap email dan pesan instan yang tidak diminta.
i. Berhati-hati ketika login yang meminta hak Administrator. Cermati alamat URL-nya yang ada di address bar.
j. Melakukan back up data.

Menurut Tabrani (2024) upaya yang dapat dilakukan korban jika terlanjur mengklik link atau pop up otomatis, yakni:

a. Mematikan data seluler.
b. Hapus riwayat browser internet.
c. Bersihkan cache penyimpanan perangkat.
d. Ubah kata sandi.
e. Kumpulkan bukti-bukti serangan phising.
f. Laporkan tindakan phising.

Phishing adalah salah satu bentuk kejahatan siber yang dilakukan dengan cara menipu korban yang dilakukan oleh hacker untuk mendapatkan informasi pribadi atau sensitif seperti kata sandi, nomor kartu kredit, dan data pribadi lainnya. Serangan phishing ini dapat terjadi melalui berbagai saluran komunikasi, seperti email, pesan teks, atau bahkan media sosial. Dampak-dampak yang ditimbulkan oleh phishing bisa sangat merugikan baik bagi individu, organisasi, maupun masyarakat secara keseluruhan.

Berikut adalah penjelasan dampak-dampak yang timbul akibat phishing secara lengkap:

1. Pencurian Informasi Pribadi dan Sensitif
   Salah satu tujuan utama dari serangan phishing adalah untuk mencuri informasi pribadi dan sensitif korban. Ini bisa mencakup:
   a. Data login seperti username dan password untuk akun email, akun media sosial, atau akun perbankan online.
   b. Informasi keuangan, termasuk nomor kartu kredit, nomor rekening bank, dan informasi pembayaran lainnya.
   c. Informasi pribadi seperti nomor identitas, alamat rumah, dan tanggal lahir.

Dengan mengakses data ini, pelaku phishing dapat melakukan tindak kejahatan lebih lanjut, seperti pencurian identitas atau penipuan keuangan.

2. Kerugian Finansial
   Phishing sering kali digunakan untuk mencuri uang dari korban. Beberapa dampak finansial yang mungkin terjadi antara lain:
   a. Penarikan dana secara ilegal: Jika informasi rekening bank atau kartu kredit dicuri, pelaku bisa mengakses dana korban dan melakukan transaksi atau transfer uang tanpa izin.
   b. Pembelian barang atau layanan secara tidak sah: Pelaku phishing bisa melakukan pembelian barang atau layanan menggunakan kartu kredit atau akun korban.
   c. Biaya penggantian dan pemulihan: Selain kerugian langsung akibat pencurian, korban mungkin perlu mengeluarkan biaya untuk mengganti kartu kredit, memperbarui data pribadi, atau mengembalikan kerugian yang dialami.
3. Penyebaran Malware dan Ransomware
   Phishing sering digunakan untuk menyebarkan malware, termasuk virus, spyware, atau ransomware, dengan tujuan:
   a. Mengakses perangkat korban: Pelaku dapat menginstal perangkat lunak berbahaya yang memungkinkan mereka mengakses perangkat korban secara jarak jauh, mencuri informasi, atau melakukan aktivitas ilegal lainnya.
   b. Menonaktifkan atau merusak sistem: Ransomware, misalnya, bisa mengenkripsi data korban dan meminta uang tebusan untuk mengembalikannya.
   c. Pencurian informasi lebih lanjut: Malware yang terinstal di perangkat korban bisa digunakan untuk mengumpulkan informasi lebih lanjut tentang korban atau organisasi.

4. Kerusakan Reputasi Pribadi dan Perusahaan
    a. Reputasi pribadi: Bagi individu, menjadi korban phishing dan kehilangan data sensitif atau uang bisa merusak reputasi pribadi mereka. Misalnya, jika data pribadi mereka digunakan untuk melakukan kejahatan, hal ini bisa menurunkan kepercayaan orang lain terhadap mereka.
    b. Reputasi organisasi: Bagi perusahaan atau organisasi, serangan phishing dapat merusak reputasi mereka, terutama jika data pelanggan atau karyawan bocor. Hal ini dapat menyebabkan hilangnya kepercayaan dari pelanggan dan mitra bisnis, serta mempengaruhi kredibilitas merek. Kerusakan reputasi ini bisa berkelanjutan, bahkan setelah kerugian materi telah diperbaiki, karena konsumen mungkin ragu untuk berinteraksi dengan perusahaan yang telah terbukti tidak mampu melindungi data pelanggan mereka.
5. Akses Tidak Sah ke Sistem dan Jaringan
   Phishing bisa memberi pelaku akses ke sistem dan jaringan yang digunakan oleh organisasi atau individu. Akibatnya, dampaknya bisa sangat serius, termasuk:
    a. Pencurian data perusahaan: Pelaku bisa mengakses dan mencuri informasi sensitif perusahaan, seperti data keuangan, strategi bisnis, atau informasi pelanggan.
    b. Kerusakan pada infrastruktur IT: Pelaku phishing bisa merusak atau merusak infrastruktur teknologi informasi organisasi dengan menyebarkan malware atau merusak perangkat keras atau perangkat lunak.
    c. Mencuri hak akses karyawan: Pelaku bisa mendapatkan hak akses karyawan ke sistem internal organisasi, yang dapat membuka pintu bagi serangan lebih lanjut atau penyalahgunaan.
6. Biaya dan Waktu Pemulihan
   Menghadapi dampak phishing biasanya membutuhkan waktu dan biaya yang signifikan untuk pemulihan, baik untuk individu maupun organisasi. Beberapa aspek pemulihan yang memerlukan waktu dan biaya termasuk:
    a. Penggantian data yang hilang: Untuk individu, ini bisa mencakup pemulihan informasi akun, penggantian kartu kredit, atau memperbarui dokumen identitas. Untuk organisasi, ini bisa mencakup perbaikan sistem yang terkena dampak dan pemulihan data yang hilang.
    b. Penanganan masalah hukum: Beberapa serangan phishing bisa melibatkan tindak pidana, yang mengarah pada kebutuhan untuk melibatkan otoritas hukum. Biaya untuk melibatkan pengacara atau menanggapi tuntutan hukum bisa sangat tinggi.

c. Perbaikan infrastruktur IT: Organisasi mungkin harus memperbaiki infrastruktur IT mereka, memasang perangkat lunak keamanan baru, atau meningkatkan sistem mereka untuk mencegah serangan di masa depan.

7. Stres dan Kerugian Psikologis
   Dampak psikologis dari menjadi korban phishing bisa sangat besar. Beberapa akibat psikologis yang mungkin dirasakan korban antara lain:
   a. Kecemasan dan stres: Korban phishing sering merasa cemas dan tertekan karena merasa privasi dan keamanannya dilanggar.
   b. Kehilangan kepercayaan diri: Terutama bagi individu, mereka mungkin merasa kehilangan kendali atas kehidupan digital mereka dan menjadi lebih waspada atau takut untuk beraktivitas online.
   c. Frustrasi: Proses pemulihan dari serangan phishing bisa memakan waktu lama dan penuh frustrasi, karena korban harus berurusan dengan bank, lembaga keuangan, atau penyedia layanan untuk mengembalikan data yang hilang.
8. Pengaruh Sosial
   Selain dampak pribadi dan finansial, phishing juga dapat memengaruhi hubungan sosial dan bisnis:
   a. Hubungan dengan keluarga atau teman: Jika informasi pribadi korban dicuri dan digunakan untuk penipuan, ini bisa merusak hubungan pribadi karena korban merasa terisolasi atau dilanggar.
   b. Hubungan bisnis: Dalam konteks bisnis, kebocoran data pelanggan akibat serangan phishing dapat merusak hubungan bisnis dengan klien atau mitra, yang mengarah pada hilangnya kesempatan kerja sama atau bisnis.

Phishing adalah ancaman serius yang dapat menimbulkan dampak jangka pendek dan jangka panjang bagi individu maupun organisasi. Untuk itu, pencegahan melalui kesadaran, edukasi, dan langkah-langkah perlindungan seperti penggunaan otentikasi dua faktor (2FA), perangkat lunak keamanan, serta kebijakan perlindungan data yang ketat sangat penting untuk mengurangi risiko dan dampak dari serangan phishing.

Yuridiksi Ciber

Prinsip yuridiksi ciber setiap negara berbeda-beda karena bergantung norma, hukum, dan etika. Menurut Masaki Hamano prinsip umum dari yuridiksi siber adalah kekuatan pemerintah dalam menjalankan wewenang atas semua orang yang berada dalam negaranya atau wilayahnya, Edy santoso (2023), yang berarti setiap Keputusan peradilan tergantung dari letak domisili negara tersebut berada.

Untuk negara Indonesia sendiri undang-undang yang mengatur tentang kejahatan phising adalah undang-undang nomor 1 tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE) yang berbunyi "Setiap Orang dengan sengaja atau mentransmisikan Informasi Elektronik atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik". Pasal 45 ayat 1 "Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan atau membuat dapat diaksesnya Informasi Elektronikmatau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (ll dipidana dengan pidana penjara paling lama 6 (enam) tahun atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah)".

Namun dalam pasal 67 ayat 1 dan ayat 3 undang-undang nomor 27 tahun 2022 mengatur lebih khusus tentang perlindungan data pribadi dan sanksi bagi pelaku kejahatan phising. Menurut Erlina Maria Christin Sinaga perlidungan data pribadi merupakan hak konstitusi yang harus di penuhi oleh pemerintah sesuai dengan peraturan perundang-undangan. Undang-undang Republik Indonesia Nomor 8 tahun 1999 tentang Perlindungan Konsumen mengatur prinsip dasar untuk memberikan perlindungan konsumen terutama pasal 4 mengatur hak-hak konsumen yang mencakup hak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan atau jasa, dan hak untuk mendapatkan pembinaan dan Pendidikan konsumen. Menurut Edy Santoso (2023)

1. Hak untuk Memperoleh Keamanan (Right to Safety)
   Terkait kejahatan phising sangat di tekankan adalah perilaku pengguna itu sendiri, yaitu kebiasaan menjaga kerahasiaan data keuangan pribadi, dan mempelajari serta memahami domain asli Lembaga yang menangani pelanggan. Informasi-informasi palsu yang terus dikirimkan melalui email dan sms serta whatsapp dapat menjadi perantara masuknya link phising dan mengetahui data pribadi serta keuangan pengguna handphone.
2. Hak untuk Memperoleh Edukasi (Right to be Education)
   Penyedia Sitem Elektronik memberikan edukasi kepada konsumen tentang bahaya dan bagaimana modus operandi kejahatan phising sehingga dapat mengurangi jumlah korban pencurian data dan kerugian secara finansial. Ini diatatur pasal 28 Peraturan Pemerintah transaksi elektronik yang menyebutkan bahwa penyelenggara system elektronik wajib melakukan edukasi kepada pengguna system elektronik.

Jadi undang-undang tersebut menekankan bahwa sebagai seorang konsumen berhak mendapatkan perlindungan sesuai dengan undang-undang nomer 8 tahun 1999. Hak yang paling mendasar adalah hak untuk di edukasi tentang bahaya kejahatan ciber dan mengenali pola-pola hacker dalam melancarkan aksinya sehingga konsumen dapat memproteksi dirinya sehingga tidak menjadi korban phising. Konsumen juga berhak mendapatkan perlindungan rasa aman terkait kejahatan phising dari Lembaga yang menangani pelanggan, Lembaga tempat konsumen berinvestasi wajib menjaga

data pribadi konsumen dan selalu meningkatkan system keamanan dan pengawasan.

Tapi dalam prakteknya masih banyak Lembaga yang menangani pelanggan tidak mengindahkan masalah tersebut dan jarang mensosialisasikanya sehingga masih banyak korban phising berjatuhan dan semakin bertambah. Karena banyaknya teknik phising yang merugikan pengguna internet, perlu dilakukan pencegahan dan penegakan hukum terhadap pelaku phising. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (UU ITE) mengatur tindakan cybercrime di Indonesia. Menurut Pasal 35 UU ITE, pelaku cybercrime metode phising dapat diancam dengan Pasal 28 ayat (1) karena termasuk dalam perbuatan membohongi pengguna untuk mendapatkan informasi dari situs web yang sebenarnya. Pisher menipu pengguna dan mengarahkan mereka ke situs web yang tidak asli yang meminta data pengguna diberikan kepada pisher. Dengan demikian, pisher mengambil keuntungan dari data pribadi dan merugikan pengguna yang datanya bocor.

KESIMPULAN DAN REKOMENDASI

Phising adalah salah satu kejahatan cyber crime dunia maya yang menggunakan teknologi modern dengan cara mengambil data-data pribadi korban untuk keuntungan pribadi. Tujuanya beragam dan yang paling umum adalah kerugian secara finansial korban. Metode yang di pakai oleh para hacker adalah memanipulasi korban dengan cara menjadi orang terpercaya atau institusi yang berwenang menggunakan suatu situs palsu yang memiliki tampilan yang sama namun berbeda URL. Hacker kemudian mengirimkan link situs palsu ini kepada target agar login ke situs tersebut dengan menggunakan kredensialnya dan tanpa disadari ia telah mengirimkan username atau passwordnya kepada hacker tersebut. Untuk mengelabui targetnya hacker mengirimkan SMS yang berisi penipuan bahwa akan mendapatkan hadiah, dana pinjaman, SMS dari Bank, dan lain sebagainya.

Untuk menghindari kejahatan phising ini yang perlu diperhatikan adalah perilaku pengguna itu sendiri, yaitu kebiasaan menjaga kerahasiaan data keuangan pribadi, dan mempelajari serta memahami domain asli Lembaga yang menangani pelanggan. Informasi-informasi palsu yang terus dikirimkan melalui email dan sms serta whatsapp dapat menjadi perantara masuknya link phising dan mengetahui data pribadi serta keuangan pengguna handphone. Yang tidak kalah penting adalah peran serta negara dalam mensosialisasikan modus operandi kejahatan phising sehingga dapat mengurangi jumlah korban pencurian data dan kerugian secara finansial.

PENELITIAN LANJUTAN

Setiap penelitian memeiliki keterbatasan; dengan demikian, Anda dapat menjelaskannya di sini dan secara singkat memberikan saran untuk penelitian lebih lanjut.

UCAPAN TERIMA KASIH

Bagian ini memberi Anda kesempatan untuk menyampaikan terima kasih kepada rekan-rekan Anda yang memberikan saran untuk makalah Anda. Anda juga dapat menyampaikan penghargaan Anda atas bantuan keuangan yang Anda terima, dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. Jurnal Komunitas Yustisia, 4(2).

Edy Santoso (September 2023) Perlindungan Konsumen Atas Kejahatan Phissing di Yuridiksi Dunia Maya.

Edy Santoso, (september 2023) Perlindungan Konsumen Atas Kejahatan Phissing di Yuridiksi Dunia Maya.

Edy Santoso, Perlindungan Konsumen Atas Kejahatan Phissing di Yuridiksi Dunia Maya, (2023).

Erlina Maria Christin Sinaga, Formulasi Legislasi Perlindungan Data Pribadi, Jurnal RechtVinding, 9.2 (2020).

Hariyono, A. G., & Simangunsong, F. (2023). Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing cybercrime) Dalam Perspektif Kriminologi. Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance, 3(1).

Indrajit, 2016 Keamanan Informasi dan Internet. Yogyakarta: Preinexus.

Luthfi Hazanatin Zahro (tahun 2023) Pengaruh Penggunaan Mobile Banking dan Perlindungan Nasabah Terhadap Cybercrime di Kota Surakarta https://bakrie.ac.id/articles/599-kenalan-dengan-5-jenis-jenis-phising-yang-patut-diwaspadai.html.

Richardus Eko Indrajit, Konsep dan Strategi Keamanan Informasi di Dunia Cyber, (Yogyakarta: Graha Ilmu, 2014).

Sabrina Tabrani , Vivi Safitri , Putu Audy Nayla P , Asmak Ul Hosnah (januari 2024) Kejahatan Phising ditinjau dari perspektif hukum dan kejahatan siber.

Saputra Gulo, A., Lasmadi, S., & Nabawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal Of Criminal, 1(2).

Undang-undang nomor 1 tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE).

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

Undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi.

Undang-undang Republik Indonesia Nomor 8 tahun 1999 tentang Perlindungan Konsumen.