Civilia :
Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan
http://jurnal.anfa.co.id

Bulan,1Tahun 2024
Vol 3 , No 1 .
1-13

KEJAHATAN PHISHING DITINJAU DARI PERSPEKTIF HUKUM DAN KEJAHATAN SIBER

Sabrina Tabrani[1], Vivi Safitri[2], Putu Audy Nayla P[3], Asmak Ul Hosnah[4]
Fakultas Hukum Universitas Pakuan, Jalan Pakuan No. 1 Bogor 16143, Indonesia [1234]

Alamat e-mail : tabranisabrina@gmail.com [1], vivisafitri950@gmail.com [2], naylahsn14@gmail.com [3], asmak.hosnah@unpak.ac.id [4]

Abstract

Phishing is the attempt to get personal information about an individual by using deception techniques. The three types of data that make up a penipuan's sasaran are private data (name, address, and email address), login data (password and username), and financial data (credit card number, account information). An irresistible penipuan is phishing, which comes from the English word "fishing". Phishing aims to trick people so that they would obediently provide private information without disclosing it, information that is provided will be used for criminal purposes. There are a lot of people that get upset when they use a suspicious website or email account. Data that is obtained in a confidential manner can be used to identify fraud or alternatively sold to other organizations to conduct non-religious transactions, such as opening bank accounts, with the primary purpose being money laundering.

Article History
Submitted 30 desember 2023
Accepted 4 januari 2024
Published 5 Januari 2024

Key Words
Law, Cyber Crime, Phishing

Abstrak

Phishing adalah upaya memperoleh informasi mengenai data seseorang dengan menggunakan teknik menipu. Data yang menjadi sasaran penipuan adalah data pribadi (nama, umur, alamat), data rekening (username dan password) dan data keuangan (kartu kredit, informasi rekening). Istilah resmi untuk penipuan adalah phishing, yang berasal dari kata bahasa Inggris "*fishing*". Phishing berupaya mengelabui orang agar secara sukarela memberikan informasi pribadi tanpa menyadarinya, informasi yang dibagikan akan digunakan untuk tujuan kriminal. Dengan menggunakan website atau email palsu yang meyakinkan, banyak orang yang tertipu. Informasi data yang diperoleh secara curang dapat langsung digunakan untuk menipu korban atau bisa juga dijual kepada pihak lain untuk melakukan tindakan tidak bertanggung jawab seperti penyalahgunaan akun, dengan sektor keuangan yang menjadi sasaran utama.

Sejarah Artikel
Submitted 30 desember 2023
Accepted 4 januari 2024
Published 5 Januari 2024

Kata Kunci
Hukum, Kejahatan Siber, Pengelabuan

Pendahuluan

Keberadaan internet dan perangkat elektronik telah menjadi bagian integral dari era modern saat ini. Orang-orang tidak hanya menggunakan internet sebagai alat untuk mencari informasi, tetapi juga sebagai sarana untuk memperluas jejaring sosial dan mencari popularitas. Platform-platform seperti Facebook, Twitter, Instagram, Snapchat, dan banyak lagi menjadi tempat di mana orang-orang terhubung, berbagi pengalaman, dan menciptakan identitas digital mereka. Selain itu, fenomena toko online juga semakin berkembang, dimana bisnis dapat

dijalankan tanpa kehadiran fisik melalui media sosial. Meningkatnya penggunaan jejaring sosial dan ketergantungan pada internet juga membawa dampak negatif, terutama dalam bentuk kejahatan siber. Dalam upaya untuk mencapai popularitas atau keuntungan, beberapa individu tidak bermoral menggunakan berbagai cara untuk menipu orang lain, dan salah satu metode yang paling umum digunakan adalah phishing.

Phishing merupakan bentuk penipuan online di mana pelaku mencoba untuk mendapatkan informasi rahasia atau sensitif dari korban dengan menyamar sebagai entitas tepercaya. Modus operandi ini dapat terjadi melalui email, situs web palsu, atau pesan palsu yang dikirimkan melalui berbagai platform. Dengan memanfaatkan daya tarik atau ketertarikan korban, pelaku phishing menciptakan ilusi keamanan atau kepentingan pribadi untuk mengelabui mereka sehingga mereka secara tidak sengaja memberikan informasi yang berharga. Fenomena phishing tidak hanya menjadi ancaman lokal, tetapi juga menyebar secara global seiring dengan perkembangan teknologi. Dalam konteks Indonesia, kejahatan dunia maya menjadi masalah yang semakin berkembang. Salah satu bentuk kejahatan siber yang paling umum di Indonesia adalah phishing. Pelaku kejahatan ini seringkali menggunakan email atau situs web palsu untuk mengecoh orang agar memberikan informasi rahasia seperti username, password, atau bahkan nomor kartu kredit.

Saat ini, penggunaan media sosial tidak hanya terbatas pada interaksi personal, tetapi juga menjadi sarana utama untuk bisnis online. Toko online memanfaatkan keberadaan media sosial untuk mempromosikan produk, berinteraksi dengan pelanggan, dan mengelola transaksi. Sistem pembayaran elektronik seperti Qris, Dana, Gopay, dan ShopeePay semakin populer karena memberikan kemudahan dan kecepatan dalam proses pembayaran. Namun, dengan kemudahan ini juga muncul risiko keamanan, dan pelaku kejahatan siber cenderung memanfaatkannya. Penting untuk memahami bahwa kejahatan siber, khususnya phishing, bukan hanya ancaman terhadap individu tetapi juga terhadap keamanan nasional dan stabilitas ekonomi. Oleh karena itu, diperlukan upaya bersama dari pemerintah, perusahaan, dan individu untuk melindungi diri dari ancaman ini.

Salah satu cara untuk melawan phishing adalah dengan peningkatan kesadaran dan pendidikan masyarakat. Semakin banyak orang yang mengetahui cara mendeteksi upaya phishing, semakin sulit bagi pelaku kejahatan untuk mencapai tujuannya. Kampanye edukasi yang menyasar pengguna internet, baik yang baru maupun yang berpengalaman, dapat membantu mengurangi tingkat keberhasilan upaya phishing.

Selain itu, pengembangan dan implementasi teknologi keamanan yang canggih juga sangat penting. Perusahaan dan penyedia layanan online harus secara terus-menerus meningkatkan sistem keamanan mereka untuk mendeteksi dan mencegah serangan phishing. Sistem keamanan yang kuat dapat melibatkan penggunaan teknologi kecerdasan buatan, analisis perilaku, dan enkripsi data untuk melindungi informasi sensitif.

Pemerintah juga memiliki peran penting dalam mengatasi kejahatan siber, termasuk phishing. Penegakan hukum yang ketat terhadap pelaku kejahatan siber dapat menjadi deterjen yang efektif. Selain itu, kerja sama antara pemerintah, sektor swasta, dan lembaga internasional dapat memperkuat pertahanan terhadap ancaman phishing secara lebih efisien.

Di tingkat individu, ada beberapa langkah yang dapat diambil untuk melindungi diri dari serangan phishing. Pertama, selalu periksa legitimasi sumber informasi atau tautan sebelum memberikan informasi pribadi. Hindari mengklik tautan atau membuka lampiran dari sumber yang tidak dikenal atau mencurigakan. Kedua, perbarui dan perkuat kata sandi secara teratur, gunakan kombinasi huruf, angka, dan karakter khusus, dan hindari menggunakan kata sandi yang mudah ditebak. Penting juga untuk selalu memperbarui perangkat lunak keamanan, termasuk antivirus dan perangkat lunak anti-malware, untuk memastikan perlindungan yang optimal. Jangan ragu untuk melaporkan kejadian phishing kepada penyedia layanan atau lembaga yang berwenang agar tindakan penegakan hukum dapat diambil.

Dalam menghadapi ancaman phishing, kolaborasi antara semua pemangku kepentingan menjadi kunci. Hanya dengan upaya bersama dari pemerintah, perusahaan, dan masyarakat dapat kita menciptakan lingkungan online yang lebih aman dan terjamin. Keberlanjutan pertumbuhan teknologi harus diimbangi dengan peningkatan kesadaran dan tindakan proaktif untuk melindungi diri dari kejahatan siber.

Metode Penelitian

Penelitian hukum adalah proses menganalisis secara mendalam tentang masalah hukum yang diselesaikan dengan meliputi metode, sistematika dan pemikiran tertentu. Studi kasus ini menggunakan penelitian yang bersifat normatif. Penelitian hukum normatif mengacu pada norma hukum yang terdapat dalam berbagai peraturan perundang-undangan yang bersifat konseptual dan sistematis. Penelitian ini dilakukan dengan menelaah dan memahami peraturan perundang-undangan serta memahami implikasi positivisasi asas-asas umum pemerintahan yang baik.

Tujuan dari penelitian ini adalah untuk menganalisis alasan mengapa kejahatan phishing sering terjadi di dunia maya dan bagaimana upaya pencegahan yang dapat dilakukan untuk mengurangi kejahatan phishing. Penelitian ini juga menggunakan penelitian normatif dengan pendekatan konseptual.

Hasil Penelitian dan Pembahasan

1. Pengertian Phishing

Phishing merupakan tindakan yang dapat mengancam atau menjebak seseorang dengan kata lain, menipu seseorang. Dengan cara mengirimkan pesan, email atau situs web palsu untuk mengelabui orang agar memberikan informasi rahasia seperti

username dan *password* atau kata sandi dan nomor kartu kredit. Sehingga korban secara tidak langsung memberikan semua informasi yang dibutuhkan pelaku. Tujuan phishing yakni untuk memperoleh keuntungan pribadi dengan melakukan pencurian dan penipuan identitas.

2. Ciri – Ciri Phising

Ancaman keamanan data pribadi semakin meningkat yang mengharuskan kita untuk waspada terhadap taktik manipulatif dari kejahatan cyber. Maka dari itu, kita perlu mengenali ciri-ciri umum phising untuk mengindari diri dari kejahatan tersebut, berikut ciri – cirinya[1] :

1. Email atau pesan tidak diinginkan
2. Alamat email atau URL yang seolah-olah resmi
3. Ancaman atau tekanan darurat
4. Permintaan informasi pribadi
5. Tautan ke situs web yang mencurigakan
6. Kesalahan tata bahasa atau ejaan yang menyolok
7. Tidak ada informasi kontak yang Jelas
8. Perasaan terlalu bagus untuk menjadi kenyataan, seperti tawaran yang terlalu menggiurkan untuk menarik perhatian Anda.
9. Spoofing dan teknologi pemalsuan
10. Identitas pengirim yang disamarkan

3. Jenis – Jenis Phising

Phishing merupakan kejahatan yang memiliki motif dan sudah direncanakan terlebih dahulu, sehingga kita dapat melihat jenis-jenis kejahatan ini[2] :

1. Phishing Scam:

   Pelaku kejahatan cyber berusaha mengelabui Anda dengan memberikan informasi pribadi seperti password, nomor rekening bank, dan nomor kartu kredit. Mereka biasanya mengirimkan file atau link yang dimodifikasi atau mengandung malware, sehingga mereka dapat menggunakan informasi ini untuk membobol akun Anda, mencuri uang, dan melakukan transaksi. Serangan phising biasanya dilakukan melalui telepon, email, SMS, atau media sosial.
2. Phishing tanpa pengenal:

   Ini adalah jenis phishing yang paling umum. Serangan ini menggunakan metode tunggal, yaitu email atau pesan massal. Karena pesan dikirim ke banyak

[1] Moh. Afaf El Kurniawan, "Ciri-Ciri Phising dan Tips Cara Mendeteksi Upaya Penipuan Online", Narasi.tv, d iakses tanggal 03 Januari 2024, https://narasi.tv/read/narasi-daily/ciri-ciri-pishing
[2] Faradilla A, "Apa itu Phising? Pengertian, Jenis, dan Cara Mengenalinya", Hostinger, di akses pada tanggal 10 November 2023 https://www.hostinger.co.id/tutorial/phising-adalah#1_Scam_Phising

orang sekaligus, fitur utama dari penipuan jenis ini adalah tidak menyebutkan nama penerima tertentu.

3. Phishing dengan Spear:

   Istilah "spear" berasal dari kata "spear", yang berarti tombak. Serangan ini ditujukan pada kelompok organisasi tertentu yang mencoba mengelabuhi korban dengan mendapatkan informasi penting, file rahasia, atau data keuangan. Serangan ini biasanya ditujukan kepada kelompok tertentu seperti pejabat pemerintah, pelanggan perusahaan, atau bahkan satu orang.

4. Phishing Kloning:

   Jenis penipuan ini terjadi dengan mengkopi situs web asli untuk mengelabui pengguna. Dalam kasus phishing web, korban biasanya diminta untuk memasukkan informasi pribadi mereka pada kolom yang disediakan, meskipun pada akhirnya kolom ini akan dikirim ke penjahat. Setelah itu, pengguna akan diarahkan ke halaman asli tanpa menyadari bahwa mereka telah tertipu oleh phishing.

5. Memancing:

   Istilah ini berasal dari kata Inggris "whale", yang berarti paus dalam bahasa Inggris. Karena hubungannya dengan memancing, jenis phishing ini menyasar korban yang lebih besar daripada orang normal. Pejabat eksekutif tingkat tinggi atau orang terkenal, seperti direktur perusahaan, biasanya menjadi sasaran penghilangan untuk mengganggu kantor mereka. Serangan ini biasanya dilakukan dengan menyamar sebagai staf pengadilan atau mengeluarkan pengumuman tentang masalah internal perusahaan.

6. Penipuan Phishing:

   Penjahat melakukan serangan phishing dengan menggunakan suara, atau suara, untuk memulai serangan dan mencari korban. Penipuan telepon biasanya membuat orang takut dengan mengatakan bahwa pelaku adalah keluarga atau kerabat korban, bahwa ada kecelakaan, atau bahkan bahwa korban mendapatkan hadiah undian. Korban akhirnya akan dimintai uang. Pelaku phishing kadang-kadang menggunakan nomor telepon atau VoIP yang tidak valid untuk menyembunyikan identitas mereka.

7. Pharming:

   Adalah jenis serangan siber di mana pelaku mengarahkan pengguna internet ke situs web yang ingin mereka kunjungi tetapi dialihkan ke situs web yang berbeda yang palsu. Serangan ini bertujuan untuk mengumpulkan data pengguna seperti password, nomor akun, nomor keamanan sosial, dan sebagainya. Hacker biasanya mengirimkan kode palsu melalui email dengan tujuan menginstal virus atau trojan pada komputer pengguna. Kemudian kode tersebut mengubah file komputer untuk mengarahkan lalu lintas lebih jauh ke

situs web yang diinginkan pengguna dan mengalihkan pengguna ke situs web palsu.

8. Smishing:

   Phishing dilakukan melalui SMS. Ketika kata-kata dikirim melalui SMS, orang yang menerimanya biasanya harus melakukan sesuatu. Selain itu, serangan ini adalah yang paling umum di Indonesia, di mana pelaku meminta korban untuk membayar dengan janji bahwa mereka akan memenangkan lotre, hadiah undian, atau uang besar.

4. Dasar Hukum Pengaturan Kejahatan *Phishing*

Pengaturan mengenai tindak pidana *cybercrime phising* diatur dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penelitian ini dilatarbelakangi oleh maraknya kasus phishing di Indonesia dikarenakan perkembangan IPTEK. Menurut data yang diperoleh Badan Siber dan Sandi Negara (BSSN) ada Tahun 2022 terdapat 164.131 kasus *email phishing* di Indonesia. Dengan jumlah paling banyak berasal dari *email* pribadi yakni 59.210 kasus[3].

Setiap tahunnya masih ada kasus phishing yang belum terselesaikan. Maka penelitian ini bertujuan untuk mengetahui penegakan hukum terhadap tindak pidana Cybercrime dengan metode Phishing dihubungkan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, untuk mengetahui kendala dan bagaimana upaya dalam mengatasi kendala penegakan hukum terhadap tindak pidana Cybercrime dengan metode Phishing di Indonesia.

Permasalahan tindak pidana cybercrime dengan metode phishing kemudian dihubungkan dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta disusun dan dianalisis menggunakan teori penegakan hukum yang menghasilkan menghasilkan gambaran penelitian ini.

Penelitian ini mendalami permasalahan serius terkait kejahatan cybercrime melalui metode phishing di Indonesia. Pengaturan hukum terkait hal ini tertuang dalam Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Latar belakang penelitian ini muncul seiring meningkatnya kasus phishing di Indonesia yang dipicu oleh pesatnya perkembangan teknologi informasi dan komunikasi.

[3] Sarnita Sadya, "Ada 164.131 Kasus Email Phising di Indonesia pada 2022", dataindonesia,di akses pada tanggal 28 Desember 2023, https://dataindonesia.id/internet/detail/ada-164131-kasus-email-phising-di-indonesia-pada-2022,

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) pada Tahun 2022, tercatat 164.131 kasus email phishing di Indonesia, di mana 59.210 di antaranya berasal dari email pribadi. Angka ini mencerminkan tingginya tingkat kejahatan cybercrime, khususnya melalui metode phishing. Namun, masih terdapat kasus-kasus phishing yang belum terselesaikan setiap tahunnya. Penelitian ini bertujuan untuk mengeksplorasi implementasi penegakan hukum terhadap kejahatan cybercrime melalui metode phishing, terutama dalam kerangka Undang-Undang Nomor 19 Tahun 2016. Selain itu, penelitian ini ingin mengidentifikasi kendala yang dihadapi dalam penegakan hukum dan menggambarkan upaya yang telah atau dapat dilakukan untuk mengatasi masalah tersebut.

Undang-Undang Nomor 19 Tahun 2016 menjadi landasan hukum untuk menanggapi kejahatan cybercrime, termasuk kasus phishing. Fokus penelitian ini adalah bagaimana Pasal 35 dalam undang-undang tersebut diterapkan dalam menanggapi kasus phishing. Metode analisis hukum digunakan untuk menghubungkan masalah tindak pidana cybercrime melalui metode phishing dengan Undang-Undang Nomor 19 Tahun 2016. Teori penegakan hukum juga diterapkan untuk memahami lebih dalam bagaimana penegakan hukum dilakukan dalam kasus ini.

Identifikasi kendala dilakukan melalui wawancara dengan pihak terkait, seperti aparat penegak hukum, perwakilan BSSN, dan ahli hukum. Hal ini bertujuan untuk menemukan faktor-faktor yang menghambat penegakan hukum terhadap kejahatan cybercrime melalui metode phishing. Beberapa kendala yang mungkin termasuk kurangnya keahlian teknis di kalangan aparat penegak hukum, keterbatasan sumber daya, dan kesulitan melacak pelaku kejahatan. Setelah mengidentifikasi kendala, penelitian ini akan menggambarkan upaya yang telah atau dapat dilakukan untuk mengatasi masalah tersebut. Upaya ini termasuk peningkatan pelatihan bagi aparat penegak hukum dalam bidang teknologi informasi, alokasi sumber daya yang lebih memadai, dan kolaborasi antar pihak terkait untuk meningkatkan efektivitas penegakan hukum.

Harapannya, hasil penelitian ini memberikan gambaran komprehensif tentang penegakan hukum terhadap kejahatan cybercrime melalui metode phishing di Indonesia. Implikasinya diharapkan menjadi dasar bagi pemerintah dan lembaga terkait untuk merumuskan kebijakan yang lebih efektif dalam menanggapi ancaman kejahatan cybercrime yang terus berkembang.

5. Dampak yang Dapat Ditimbulkan

Di era digital yang semakin pesat, ancaman terhadap keamanan data pribadi semakin meningkat. Ancaman dan dampak yang sangat merugikan ini dapat mengancam keselamatan seseorang adalah ancaman kejahatan phishing. Kejahatan ini dapat menimbulkan berbagai dampak negatif bagi korbannya, antara lain :

1. Kehilangan akses akun pribadi : hal ini mengakibatkan hilangnya data penting, dana, atau informasi yang bersifat pribadi milik korban.[4]
2. Kerugian finansial: Serangan phishing dapat menyebabkan kehilangan uang secara langsung, seperti kehilangan uang atau barang berharga, atau kehilangan uang secara tidak langsung, seperti biaya hukum dan biaya keamanan siber.
3. Merusak reputasi perusahaan : serangan ini mengakibatkan kerugian finansial dan kehilangan kepercayaan pelanggan.[5]
4. Dampak psikologis: Serangan phishing dapat menyebabkan trauma emosional yang signifikan, seperti perasaan frustrasi, takut, marah, tidak berdaya, malu, depresi, dan gangguan tidur. Karena tidak dapat memperoleh identitas baru seperti pencurian identitas yang mungkin lebih berbahaya bagi korban, selain korban phishing mungkin mengalami serangan psikologi karena orang lain yang menyalahkan mereka karena terkena serangan phishing[6].

Mengenali indikasi email atau situs web phishing, seperti kesalahan ejaan mencolok, tautan yang mencurigakan, atau permintaan informasi pribadi yang tak lazim, sangat penting sebagai langkah awal untuk menghindari dampak negatifnya. Mencegah efek buruk dari aktivitas phishing menjadi krusial karena dapat berujung pada pencurian identitas, kehilangan data pribadi, atau bahkan kerugian finansial yang signifikan. Oleh karena itu, pemahaman akan cara-cara untuk mengenali upaya phishing dan melindungi informasi pribadi menjadi aspek yang sangat penting dalam menjaga privasi dan keamanan data.

Namun, tindakan pencegahan tidak hanya sebatas pada pengenalan tanda-tanda phishing. Mencegah kerentanan yang bisa dimanfaatkan oleh pelaku cybercrime juga menjadi prioritas utama. Salah satu langkah penting adalah dengan menggunakan kata sandi yang kompleks dan sulit ditebak untuk akun-akun daring. Kata sandi yang kuat terdiri dari campuran karakter, seperti huruf besar dan kecil, angka, serta simbol khusus, sehingga menjadi sulit bagi pihak yang tidak berwenang untuk menebak atau meretasnya.

Selain itu, selalu menjaga perangkat lunak dalam kondisi terupdate juga merupakan hal yang sangat penting. Pembaruan perangkat lunak secara teratur seringkali mencakup perbaikan atas kerentanan keamanan yang mungkin dieksploitasi

[4] Fakultas Ilmu Komputer Universitas Esa Unggul, "Fenomena Phising : Ancaman yang Merugikan dan Mengancam Keselamatan Online Anda", di akses pada 03 Januari 2024, https://fasilkom.esaunggul.ac.id/fenomena-phising-ancaman-yang-merugikan-dan-mengancam-keselamatan-online-anda/

[5] Literasi Keamanan Siber, "Waspada Serangan Phising", di akses pada 03 Januari 2024 https://csirt.kalbarprov.go.id/posts/phising#:~:text=Korban%20serangan%20phishing%20dapat%20kehilangan,dan%20hilangnya%20kepercayaan%20dari%20pelanggan.

[6] Prosperita IT News, "Dampak Psikologis Serangan Phising",di akses pada 03 Januari 2024, https://news.prosperita.co.id/dampak-psikologis-serangan-phising/

oleh para pelaku kejahatan cyber, sehingga mengurangi risiko serangan yang merugikan. Dengan mengaplikasikan praktik-praktik keamanan digital, seperti mengenali ciri-ciri phishing, menggunakan kata sandi yang kuat, dan rutin memperbarui perangkat lunak, individu dapat mengurangi risiko menjadi korban serangan cyber yang berpotensi merusak. Pemahaman akan praktik keamanan digital ini menjadi kunci dalam menjaga keamanan informasi pribadi dari ancaman cyber yang terus berkembang.

6. Upaya yang Dapat Dilakukan

Adapun cara-cara menurut Tim Penelitian dan Analisa Global Kaspersky Lab untuk menghindari dan melindungi diri dari Phishing adalah sebagai berikut[7] :

- Buat bookmark untuk halaman login situs sosial seperti Facebook atau ketik URL *www.facebook.com* secara langsung di *address bar browser* Anda.
- Jangan klik link di pesan email.
- Hanya ketik data rahasia di website yang aman.
- Secara teratur periksa akun bank Anda dan laporkan segala sesuatu yang mencurigakan kepada bank Anda.
- 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*.
- Menginstall *software* untuk kemanan internet dan tetap mengupdate antivirus.
- Menginstall *patch* keamanan.
- Waspada terhadap email dan pesan instan yang tidak diminta.
- Berhati-hati ketika login yang meminta hak Administrator. Cermati alamat URL-nya yang ada di *address bar*.
- Mem-*back up* data.

Upaya yang dapat dilakukan korban jika terlanjur mengklik *link* atau *pop up* otomatis, yakni :

- Matikan data seluler atau WiFi
- Hapus *history browser* internet
- Bersihkan *cache* penyimpanan perangkat
- Ubah kata sandi
- Kumpulkan bukti-bukti serangan phishing
- Laporkan tindakan phishing

[7] Kompas.com, "10 Tips Mencegah Serangan Phising", di akses pada 10 November 2023, https://tekno.kompas.com/read/2009/05/27/17001058/10.tips.mencegah.serangan.phising

- Tambahkan perlindungan pada perangkat elektronik

Ada beberapa penjelasan langkah yang dapat diambil untuk menjaga keamanan saat online:

1. Gunakan Bookmark atau Masukkan URL Langsung
   Saat ingin mengakses situs sosial seperti Facebook, lebih baik gunakan bookmark yang sudah disimpan atau ketik URL langsung di address bar. Ini mencegah akses melalui tautan dari email yang mungkin menjadi upaya phishing.
2. Hindari Klik Tautan di Email
   Lebih baik hindari mengklik tautan yang disertakan dalam pesan email. Lebih aman untuk membuka situs secara manual.
3. Data Rahasia Hanya di Situs Terpercaya
   Informasi sensitif, seperti detail login atau informasi keuangan, sebaiknya hanya dimasukkan di situs yang terjamin keamanannya.
4. Rutin Cek Akun Bank dan Laporkan Aktivitas Mencurigakan
   Melakukan pemeriksaan berkala pada akun bank dan segera memberi tahu pihak bank jika terdapat aktivitas yang mencurigakan.
5. Perhatikan Tanda-tanda Phishing dalam Email
   Waspadai pesan email yang menjanjikan hadiah atau promosi dengan ciri-ciri seperti tidak personal, diterima oleh banyak orang, atau terdapat kesalahan bahasa. Ini bisa menjadi upaya untuk menghindari deteksi sebagai phishing.
6. Pasang Software Keamanan dan Update Antivirus
   Penting untuk memasang perangkat lunak keamanan internet dan selalu mengupdate antivirus untuk melindungi perangkat dari malware.
7. Lakukan Instalasi Patch Keamanan
   Memasang update terbaru untuk menjaga perangkat dari celah keamanan yang bisa dimanfaatkan oleh penyerang.
8. Waspada terhadap Pesan yang Tak Diminta
   Hindari merespons email atau pesan instan yang tidak diminta, khususnya yang meminta informasi pribadi atau login.
9. Perhatikan Login Sebagai Administrator
   Saat diminta untuk login sebagai administrator, pastikan alamat URL yang tertera di address bar untuk memastikan keamanannya.
10. Backup Data secara Rutin
    Melakukan pencadangan data secara berkala untuk menghindari kehilangan informasi penting.

Jika sudah mengklik tautan atau pop-up yang mencurigakan, respons cepat dapat dilakukan dengan:

- Mati-kan Koneksi Data atau WiFi
Langkah awal untuk memutuskan akses dari sumber yang mencurigakan.
- Hapus Riwayat Browser dan Bersihkan Cache
Membersihkan jejak online dari perangkat.
- Ubah Kata Sandi
Segera ubah kata sandi untuk mengamankan akun.
- Kumpulkan Bukti Serangan Phishing
Simpan bukti-bukti serangan untuk tindakan lebih lanjut.
- Laporkan Tindakan Phishing
Segera laporkan ke pihak berwenang atau platform terkait.
- Tambahkan Perlindungan pada Perangkat
Perkuat perlindungan keamanan pada perangkat untuk menghindari serangan serupa di masa mendatang.

Kesimpulan

Phishing adalah jenis penipuan yang mengancam dan menjebak seseorang dengan mengirimkan pesan, email, atau situs web palsu untuk mendapatkan informasi rahasia. Ini termasuk nama pengguna, kata sandi, atau nomor kartu kredit, dengan tujuan utama untuk mencuri identitas dan mendapatkan keuntungan pribadi. Dalam menghadapi taktik manipulatif kejahatan cyber, terutama phishing. Kita harus memahami ciri-ciri phishing yang umum, seperti pesan tidak diinginkan, alamat email atau URL palsu, ancaman darurat, tautan mencurigakan, kesalahan tata bahasa, informasi kontak yang tidak jelas, penawaran yang terlalu menggiurkan, teknologi pemalsuan seperti spoofing, dan identitas pengirim yang samar. Dengan mengetahuinya, kita dapat lebih baik melindungi diri kita dari kejahatan dunia maya.

Modus dan fitur kejahatan siber ini semakin beragam dan terus berkembang. Karena itu, kita juga mempelajari berbagai jenis phishing, seperti scam phishing, blind phishing, spear phishing, clone phishing, whaling, vishing, pharming, dan smishing. Pasal 35 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur tindakan phishing di internet. Ini adalah undang-undang yang berlaku di Indonesia untuk phishing ini. Meskipun demikian, banyaknya kasus phishing menunjukkan bahwa penegakan hukum masih menghadapi tantangan. Pada tahun 2022, Badan Siber dan Sandi Negara (BSSN) mencatat 164.131 kasus phishing email di Indonesia, sebagian besar berasal dari email pribadi.

Dalam era digitalisasi, ancaman terhadap keamanan data pribadi semakin meningkat, dengan phishing menjadi penyebab utamanya. Serangan ini dapat menyebabkan kehilangan akses akun, kerugian finansial, kerusakan reputasi perusahaan, dan kerugian psikologis. Selain menjaga keamanan dengan kata sandi kuat dan pembaruan perangkat lunak, orang harus

waspada terhadap tanda-tanda phishing seperti kesalahan ejaan dan tautan mencurigakan. Langkah-langkah pencegahan ini sangat penting untuk menghindari akibat buruk di era teknologi yang semakin kompleks ini.

Upaya yang disarankan oleh Tim Penelitian Kaspersky Lab untuk menghindari serangan phishing termasuk membuat bookmark di situs sosial, menghindari mengklik link di email, dan hanya memasukkan informasi sensitif di situs web terpercaya. Proses tambahan termasuk memeriksa akun bank secara teratur, memeriksa software keamanan internet secara teratur, mengidentifikasi tanda-tanda phishing dalam email, menginstal antivirus secara teratur, dan tetap waspada terhadap email tidak diminta. Disarankan untuk mematikan data seluler, menghapus catatan browser, mengubah kata sandi, dan mengirimkan laporan dalam kasus serangan. Anda juga harus menambahkan perlindungan pada perangkat elektronik Anda. Secara keseluruhan, pedoman ini membantu mengurangi risiko dan mengurangi dampak serangan phishing.

Saran

Penelitian ini memberikan gambaran tentang penegakan hukum terhadap tindak pidana cybercrime di Indonesia dengan menghubungkan masalah phishing dengan Undang-Undang Nomor 19 Tahun 2016. Diharapkan bahwa evaluasi kendala dan upaya penegakan hukum akan menjadi dasar untuk perbaikan dan penguatan sistem hukum untuk melindungi masyarakat dari ancaman phishing di era teknologi informasi yang berkembang.

Di Indonesia, mengatasi kasus phishing membutuhkan pendekatan holistik yang melibatkan berbagai sektor. Untuk meningkatkan pertahanan terhadap serangan phishing, institusi pendidikan dan kampanye kesadaran publik tentang keamanan cyber, pelatihan karyawan, penerapan teknologi keamanan tinggi, dan kolaborasi pemerintah-swasta diperlukan.

Untuk mengurangi risiko, mekanisme pelaporan yang efektif, audit keamanan rutin, dan penanganan insiden phishing yang cepat diperlukan. Untuk memberikan perlindungan terbaik kepada korban, peraturan hukum yang kuat, termasuk hukuman yang tegas, harus diperkuat. Untuk menghadapi serangan phishing yang semakin canggih, kolaborasi internasional dan dukungan pada penelitian dan inovasi dalam solusi keamanan siber sangat penting. Dengan menerapkan langkah-langkah ini, diharapkan Indonesia dapat mengatasi serangan phishing, menjaga keamanan masyarakat, dan mengatasi masalah keamanan siber secara keseluruhan.

Daftar Pustaka

A, F. (2022, Desember 16). *Apa Itu Phising? Pengertian, Jenis, dan Cara Mengenalinya*. Retrieved from Hostinger: https://www.hostinger.co.id/tutorial/phising-adalah#1_Scam_Phising

Fakultas Ilmu Komputer Universitas Esa Unggul. (2023, Juni 12). *Fenomena Phising : Ancaman yang Merugikan dan Mengancam Keselamatan Online Anda*. Retrieved from fasilkom.esaunggul.ac.id: https://fasilkom.esaunggul.ac.id/fenomena-phising-ancaman-yang-merugikan-dan-mengancam-keselamatan-online-anda/

Kurniawan, M. A. (2023, November 9). *Ciri-Ciri Phising dan Tips Cara Mendeteksi Upaya Penipuan Online*. Retrieved from narasi.tv: https://narasi.tv/read/narasi-daily/ciri-ciri-pishing

Literasi Keamanan Siber. (n.d.). *Waspada Serangan Phising*. Retrieved from csirt.kalbarprov.go.id: https://csirt.kalbarprov.go.id/posts/phising#:~:text=Korban%20serangan%20phishing%20dapat%20kehilangan,dan%20hilangnya%20kepercayaan%20dari%20pelanggan.

M. Zaki Rizaldi, R. D. (2023). Analisis Kasus Cybercrime Dengan Studi Kasus Hacker Bjorka Terhadap Pembocoran Data. *Jurnal Justitia*, 5.

Prosperita IT News. (n.d.). *Dampak Psikologis Serangan Phising*. Retrieved from news.prosperita.co.id: https://news.prosperita.co.id/dampak-psikologis-serangan-phising/

Sadya, S. (2023, Maret 28). *DataIndonesia.id*. Retrieved from dataindonesia.id: https://dataindonesia.id/internet/detail/ada-164131-kasus-email-phising-di-indonesia-pada-2022