Jurnal Teknik Informatika (JUTIF)
Vol. 5, No. 4, August 2024, pp. 631-640

DOI: https://doi.org/10.52436/1.jutif.2024.5.4.2294
p-ISSN: 2723-3863
e-ISSN: 2723-3871

FORENSIC ANALYSIS OF PHISHING ATTACKS: INVESTIGATIVE APPROACH

Quido Conferti Kainde*[1], Josua Setdefit Tambanaung[2], Valent Tio Inkiriwang[3], Alexandra Anrala Putri Mile*[4]

[1,2,3,4]Informatics Engineering, Engineering Faculty, Universitas Negeri Manado, Indonesia
Email: *[1]quidokainde@unima.ac.id, [2]23210014@unima.ac.id,
[3]23210101@unima.ac.id,*[4]23210084@unima.ac.id

(Article received: June 14, 2024; Revision: June 19, 2024; published: August 21, 2024)

Abstract

Phishing attacks continue to pose a significant threat to cybersecurity, with perpetrators becoming increasingly sophisticated in crafting convincing fraudulent methods. This article examines the forensic analysis process used to effectively investigate phishing attacks. Through a review of existing literature, the author understands the workings of phishing and analyzes real cases that have occurred, followed by data collection using secondary sources. Using theories and insights gained from literature studies, the author analyzes and identifies important aspects of the conducted research data. A content analysis method is employed to analyze the data, determining the steps for prevention and investigation of phishing attacks. In this analysis, thematic and textual methods are applied to gather crucial components of a phishing attack. The analysis results indicate that forensic approaches and a deep understanding of phishing mechanisms can help protect data and significantly reduce the impact of phishing attacks. This article concludes by providing practical recommendations to enhance readiness in facing future phishing attacks.

Keywords: *Forensic Analysis, Forensic Investigation, Phishing Attack*

ANALISIS FORENSIK ATAS SERANGAN PHISHING: PENDEKATAN INVESTIGASI

Abstrak

Serangan phishing terus menjadi ancaman signifikan bagi keamanan siber, dengan pelaku semakin canggih dalam menyusun metode penipuan yang meyakinkan. Artikel ini mengkaji proses analisis forensik yang digunakan untuk menyelidiki serangan phishing secara efektif. Melalui tinjauan literatur yang ada, penulis memahami cara kerja phishing dan menganalisis kasus nyata yang telah terjadi, diikuti dengan pengumpulan data menggunakan sumber sekunder. Menggunakan teori dan wawasan yang diperoleh dari studi literatur, penulis menganalisis dan mengidentifikasi aspek-aspek penting dari data penelitian yang dilakukan. Metode analisis konten digunakan untuk menganalisis data, menentukan langkah-langkah pencegahan dan penyelidikan serangan phishing. Dalam analisis ini, metode tematik dan tekstual diterapkan untuk mengumpulkan komponen penting dari serangan phishing. Hasil analisis menunjukkan bahwa pendekatan forensik dan pemahaman mendalam tentang mekanisme phishing dapat membantu melindungi data dan secara signifikan mengurangi dampak serangan phishing. Artikel ini menyimpulkan dengan memberikan rekomendasi praktis untuk meningkatkan kesiapan dalam menghadapi serangan phishing di masa depan.

Kata kunci: *Forensic Analysis, Forensic Investigation, Phishing Attack*

1. PENDAHULUAN

Phishing merupakan salah satu bentuk kejahatan siber yang memerlukan perhatian serius. Serangan ini dapat menyerang siapapun tanpa memandang status sosial atau posisi, dan memiliki dampak yang meluas. Dalam taktik phishing, pelaku menggunakan trik untuk mencuri informasi pribadi seseorang[1]. Mereka menciptakan situasi palsu, seperti email, tautan, atau situs web, yang terlihat seperti berasal dari sumber yang dapat dipercaya, tujuannya adalah untuk menipu korban agar memberikan informasi sensitif, seperti nama pengguna, kata sandi, nomor kartu kredit, atau detail rekening bank[2]. Pelaku phishing sering menyamar sebagai entitas yang sah untuk menipu dan meminta korban memberikan informasi yang sensitif[3]. Berdasarkan laporan *Anti-Phishing Working Group* (APWG), serangan phishing meningkat secara global dengan ribuan email dan situs web palsu yang dilaporkan setiap bulan. Fenomena ini menunjukkan pentingnya analisis mendalam untuk memahami

karakteristik serangan phishing dan mengembangkan strategi mitigasi yang efektif.

Ancaman phishing di dunia digital sangatlah serius karena dapat mengakibatkan kerugian finansial dan pelanggaran privasi yang signifikan bagi para korban[4]-[5]. Terlepas dari dampaknya, serangan phishing secara umum tidak memerlukan banyak usaha untuk dilakukan[6]. Serangan phishing memiliki banyak bentuk dan biasanya melibatkan berbagai saluran komunikasi, seperti email, pesan instan, *quick response* (QR) *code*, dan media sosial[7]. Dengan demikian, penting untuk memahami beberapa ciri-ciri yang dapat membantu mengidentifikasi serangan phishing. Pertama, serangan phishing sering kali mengaku berasal dari lembaga atau institusi resmi, seperti bank atau pemerintah[8]. Kedua, pesan phishing biasanya menggunakan kalimat yang mengejutkan atau memaksa agar korban segera bertindak[9]. Selain itu, phisher sering menyertakan tautan palsu yang mengarah ke situs web tiruan[10], di awal tahun 2024 tercatat ada sebanyak 45 juta link phishing yang aktif[11]. Beberapa serangan phishing juga memancing korban dengan menggunakan konten pornografi[12].

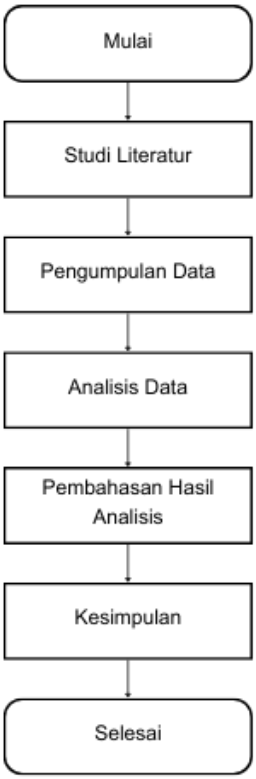
Phishing dapat menyebabkan kerugian, penting untuk selalu waspada terhadap pesan mencurigakan, hindari mengklik tautan sembarangan, dan pastikan keamanan situs web yang diakses[13]. Gunakan sistem keamanan autentikasi dua faktor (*Two-Factor Authentication*) untuk mencegah akun digunakan oleh sembarangan orang. Salah satu cara untuk mendeteksi dan mencegah serangan phishing adalah dengan menggunakan sistem *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), yang memonitor jaringan untuk aktivitas mencurigakan dan memberikan peringatan ketika potensi ancaman terdeteksi serta mengotomatisasikan tindakan untuk mencegah serangan tersebut dengan memblokir aktivitas yang mencurigakan secara otomatis[14].

Penelitian sebelumnya telah banyak membahas tentang teknik phishing dan dampaknya terhadap individu dan organisasi. Namun, terdapat kekurangan dalam pendekatan investigasi yang komprehensif. Studi oleh Alabdan menunjukkan bahwa psikologi seseorang menjadi faktor utama keberhasilan phishing[15]. Sementara itu, penelitian oleh Safi dan kawan-kawan menyoroti teknik *social engineering* yang digunakan oleh penyerang untuk menyamar sebagai entitas sah. Fokus terbaru dalam teori yang dikaji adalah pendekatan forensik dalam investigasi serangan phishing, yang melibatkan analisis komprehensif terhadap bukti digital dan komponen penyerangan untuk mengidentifikasi pelaku dan metode serangan.

Penelitian ini bertujuan untuk menganalisis serangan phishing dengan pendekatan forensik, mengidentifikasi metode dan pola serangan, serta merumuskan langkah-langkah investigasi yang efektif dalam mengidentifikasi pelaku dan mencegah serangan serupa di masa depan. Perbedaan utama pada penelitian ini dibandingkan dengan penelitian sebelumnya terletak pada pendekatan investigasi yang sistematis dan penggunaan teknik forensik yang untuk mengidentifikasi pelaku serangan phishing.

2. METODE PENELITIAN

Berikut tahapan yang penulis lewati dalam pembuatan artikel ini:



Gambar 1. Tahapan Penelitian

Tahap awal dalam penelitian ini adalah melakukan studi literatur. Studi literatur melibatkan tinjauan kritis dan evaluasi terhadap karya-karya ilmiah yang relevan dalam bidang studi yang dituju. Tujuannya adalah mengumpulkan data berupa teori atau penelitian yang dapat menjadi acuan. Studi literatur membantu memahami dan merangkum temuan sebelumnya, mengidentifikasi tren, dan memperdalam pengetahuan dalam bidang ini.

Setelah studi literatur, tahap selanjutnya adalah pengumpulan data. Penulis menggunakan metode studi kasus untuk mengumpulkan data yang relevan dengan kasus phishing yang umum terjadi. Data yang digunakan adalah data sekunder, yaitu data yang telah dikumpulkan dan diolah sebelumnya oleh peneliti atau sumber lainnya.

Kemudian, dilakukan analisis data menggunakan metode analisis konten dengan kombinasi metode analisis tekstual dan analisis tematik. Metode tekstual digunakan untuk menganalisis teks terkait serangan phishing, seperti email masuk, dan tautan palsu. Tujuannya adalah mengidentifikasi pola dalam serangan phishing.

Metode tematik digunakan untuk menganalisis pola atau tema yang muncul dari hasil analisis tekstual, dengan tujuan mengetahui motif serangan phishing dan metode yang digunakan.

Tahap akhir adalah pembahasan hasil analisis. Hasil dari analisis data digunakan sebagai pedoman untuk menentukan metode dan tahapan investigasi yang ideal untuk kasus phishing dengan pendekatan forensik.

3. HASIL DAN PEMBAHASAN

3.1. Studi Literatur

Penulis memulai penelitian dengan melakukan studi literatur untuk mengidentifikasi tren dan temuan-temuan penting terkait serangan phishing, baik serangan yang berbasis web ataupun lampiran berisi *malware*, hingga pesan palsu dari entitas yang terlihat sah. Studi kasus mencakup beberapa area utama sebagai berikut.

3.1.1. Karakteristik Serangan Phishing

Serangan phishing biasanya menyasar informasi sensitif dari pengguna, misalnya informasi pribadi atau bahkan informasi finansial seseorang. Menurut Ahmadian dan rekan-rekannya, serangan phishing seringkali mengatasnamakan perusahaan atau entitas yang sah untuk memancing pelaku memberikan informasi sensitif. Pelaku serangan phishing biasanya menggunakan trik psikologis untuk mengelabui korban. Fauzi dan rekan-rekannya menyatakan bahwa Pelaku serangan menggunakan kemampuan sosial untuk membuat pesan phishing seolah-olah terdesak dan membutuhkan tindak secepatnya dari korban.

3.1.2. Tren Teknik Serangan Phishing

Terdapat perkembangan dalam teknik penyerangan phishing, terutama teknik psikologis yang melibatkan rekayasa sosial untuk memanfaatkan kepercayaan serta kepanikan untuk mengelabui korban. Menurut Alkahlil dan rekan-rekannya, serangan phishing menggunakan kombinasi dari kemampuan sosial dan teknikal untuk menciptakan serangan yang kuat. Beberapa sumber juga mengatakan bahwa serangan phishing merupakan serangan *social-engineering* yang menyerang siapapun tanpa memandang bulu.

Evolusi teknologi memberikan peningkatan ketahanan akan serangan, namun teknik penyerangan phishing juga mengalami perubahan. Beberapa teknik seperti *malware attachment* yang dulunya sering digunakan, sekarang menjadi kurang umum dikarenakan perkembangan alat pendeteksi *malware* yang semakin canggih. Melalui beberapa literatur, penulis menemukan adanya perkembangan dalam teknik phishing. Teknik *url-email-phishing* yang ada sekarang ini telah mengalami perubahan dari yang dulunya hanya berisi *open-url*, sekarang telah berubah menjadi *pseudonym-url* atau url samaran untuk menghindari *tools* atau alat pendeteksi keamanan. Namun, dari semua literatur yang ditinjau, penulis menemukan bahwa teknik *spoofing* atau pemalsuan identitas merupakan teknik yang paling sering digunakan. Sejak dahulu teknik *spoofing* telah menjadi metode yang umum digunakan, bahkan sampai saat ini pun, teknik ini masih sangat sering digunakan dikarenakan tingkat keberhasilan yang cenderung tinggi, serta cenderung mudah untuk dilakukan, namun akan sulit diterapkan pada beberapa metode.

3.1.3. Motif dan Metode Serangan Phishing

Melalui tinjauan literatur, penulis menyadari akan pentingnya memahami motif serta metode dalam serangan phishing.

Melalui penelitian yang dilakukan Alkhalil dan rekan-rekannya, penulis menemukan bahwa motif utama dari serangan phishing adalah keuntungan finansial. Korban serangan tersebut dapat mengalami kerugian finansial yang signifikan, seperti kehilangan uang dari rekening bank, kartu kredit yang telah dicuri oleh pelaku phishing, atau bahkan keuntungan yang jauh lebih besar dari suatu perusahaan jika dilakukan dengan metode yang tepat, serta data pribadi yang dicuri juga dapat dijual secara ilegal untuk mendapat keuntungan lebih. Alkhalil dan rekan-rekannya juga menemukan bahwa perusahaan yang menjadi korban phishing dapat mengalami penurunan reputasi yang signifikan dan kehilangan kepercayaan konsumen, bahkan bisa kehilangan kepercayaan terhadap layanan online.

Melalui tinjauan literatur, penulis juga menemukan beberapa metode yang digunakan dalam serangan phishing. Dari penelitian Alkhalil dan rekan-rekannya, lebih dari 91% kasus pembobolan sistem diakibatkan serangan yang diinisiasi oleh email. Ini menunjukkan bahwa phishing berbasis email merupakan salah satu metode yang sangat umum digunakan. Sedangkan Fauzi dan rekan-rekannya mengklasifikasikan dua jenis serangan phishing, yaitu serangan berbasis komunikasi dan serangan berbasis *social-engineering*. Modus komunikasi yang sering digunakan antara lain adalah phishing berbasis email, SMS (SMiShing), dan *voice* (Vishing). Sedangkan serangan phishing berbasis *social-engineering* meliputi pendekatan *deceptive*, *spear*, dan *whaling*.

Ada pula beberapa metode yang lebih jarang digunakan termasuk *Angler Phishing*, yang menggunakan media sosial untuk menipu korban dengan akun palsu yang tampak seperti akun layanan pelanggan resmi. *Pharming* mengarahkan korban dari situs web yang sah ke situs web palsu melalui pengalihan DNS, memerlukan keahlian teknis yang lebih tinggi dan lebih sulit dideteksi oleh pengguna rata-rata. *Tabnabbing* menggunakan skrip berbahaya untuk mengubah konten tab yang tidak aktif di browser korban ke situs phishing, berharap korban akan kembali ke tab dan memasukkan informasi sensitif mereka. *Man-in-the-Middle* (MitM) phishing melibatkan penyerang yang mencegat komunikasi antara dua pihak untuk

mencuri informasi sensitif, sering kali menggunakan jaringan *Wi-Fi* publik atau tidak aman.

3.2. Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan melalui metode studi kasus yang fokus pada serangan phishing. Data yang akan digunakan adalah data sekunder yang telah dikumpulkan dan diolah sebelumnya oleh para peneliti atau sumber lainnya. Data sekunder ini diperoleh dari berbagai sumber, termasuk jurnal ilmiah, laporan keamanan siber, dan database yang mencatat insiden phishing. Tahapan yang akan dilalui dalam pengumpulan data ini termasuk identifikasi sumber dan pengumpulan data.

3.2.1. Identifikasi Sumber Data

Penulis menelusuri beberapa database publik seperti Kaggle dan *PhishTank* yang mendokumentasikan insiden phishing, serta mengakses laporan tahunan dan kuartalan dari perusahaan keamanan siber yang mencakup analisis tren serangan phishing seperti *Anti-Phishing Working Group* (APWG).

3.2.2. Pengumpulan Dataset

Dari database publik kaggle, penulis mengambil dataset mengenai email phishing, yang pertama oleh Naser dan rekannya, dan dataset mengenai URL phishing yang dikumpulkan oleh Prisha Sawhney. Sedangkan dari laporan milik *Anti-Phishing Working Group*, penulis mengambil data dari dua laporan terbaru, yaitu kuarter 4 tahun 2023 sampai kuarter 1 tahun 2024. APWG mengelompokkan data yang mereka kumpulkan menggunakan sistem kuarter, istilah kuarter atau *quarter* mengacu pada periode yang dibagi menjadi 4 periode untuk tiap tahun.

3.3. Analisis Data dan Pembahasan

Berdasarkan data dari Naser dan rekannya, penulis mendapatkan dataset yang berisi 2859 email yang dicurigai merupakan email phishing. Dari 2859 email tersebut, terdapat tiga atribut utama: *subject*, *body*, dan *label*. *label* disini hanya bisa bernilai 1 atau 0, label 1 berarti email tersebut merupakan serangan phishing, sedangkan label 0 berarti email tersebut aman dari serangan phishing.

Untuk dataset ini, penulis menerapkan metode analisis tekstual untuk mencari pola dalam subyek dan *body* atau isi dari email phishing, mengidentifikasi kata-kata tertentu yang sering muncul dalam subyek dan *body*, serta menerapkan analisis tematik untuk menentukan tujuan dari penggunaan kata atau kalimat tertentu. Berdasarkan hasil analisis, penulis mendapatkan jumlah email yang merupakan serangan phishing, serta kata-kata yang sering muncul di *subject* dan *body* email.

Tabel 1. Jumlah email phishing

Jumlah Email	Kategori
458	Tidak Aman (Phishing)
2401	Aman (Bukan Phishing)

Tabel 1 diatas menunjukkan jumlah email yang termasuk phishing dan yang tidak termasuk phishing dari total 2859 email. Sebanyak 458 email atau sekitar 16.9% dari total email merupakan email phishing. Sedangkan email yang ternyata bukan merupakan email phishing berjumlah jauh lebih banyak, yaitu sebanyak 2401 email atau sekitar 83.1% dari total email.

Dari 2.859 email yang dicurigai sebagai serangan phishing, hanya 458 email yang benar-benar merupakan serangan phishing, sedangkan 2.401 email lainnya bukan. Perbandingan jumlah ini menunjukkan bahwa tingkat kemiripan antara email phishing dan email biasa semakin tinggi. Serangan phishing terus berkembang dan menjadi semakin canggih seiring berjalannya waktu. Serangan phishing saat ini menjadi lebih sulit dideteksi dibandingkan dengan yang sebelumnya.

Dari dataset yang sama. penulis juga menemukan kata-kata dan simbol yang sering muncul dalam email phishing sebagai berikut.

Tabel 2. Kata dan simbol yang sering mucul dalam 2.859 email phishing

Kata/Simbol	Kemunculan di *Subject*	Kemunculan di *Body*
?	445	458
!	151	360
what	7	360
free	52	281
new	38	244
get	12	257
$	25	243
please	4	244
only	9	235
for you	6	213
win	7	198
what	7	184
money	8	172
offer	8	172
check	3	173

Tabel 2 di atas menunjukkan 15 kata yang paling sering muncul dari 458 email phishing, beserta frekuensi kemunculannya diurutkan secara *descending* atau dari terbesar ke terkecil.

Temuan ini menunjukkan pola penggunaan bahasa dan simbol yang sering dipakai dalam email phishing. Penggunaan simbol-simbol seperti "?" dan "!" seringkali bertujuan untuk menarik perhatian penerima email. Tanda tanya (?) digunakan untuk menimbulkan rasa ingin tahu atau kesan ketidakpastian, sedangkan tanda seru (!) digunakan untuk menekankan urgensi atau pentingnya pesan tersebut. Simbol tanda tanya yang muncul di hampir semua subjek email dan muncul di semua isi email, menunjukkan bahwa email phishing seringkali memancing calon korban dengan rasa ingin tahu dan penasaran. Kemudian simbol tanda seru yang memiliki angka kemunculan terbanyak setelah tanda tanya menunjukkan bahwa email phishing seringkali membuat bertujuan membuat calon korban menjadi panik akan kesan urgensi dari pesan email tersebut. Kata *"what"* yang termasuk ke dalam daftar tersebut juga seringkali digunakan dalam kalimat, bersamaan dengan kedua simbol tersebut untuk menciptakan kesan urgensi dan keingintahuan pada calon korban.

Lalu ada penggunaan kata-kata persuasif dan mendesak seperti *"please"*, *"only"*, dan *"for you"* memberikan kesan personal dan mendesak, seolah-olah email tersebut ditujukan khusus untuk penerima dan membutuhkan tindakan segera. Sedangkan kata-kata memikat seperti *"free"*, *"win"*, *"money"*, *"want"*, dan *"offer"* digunakan untuk memancing minat dan menimbulkan rasa ingin memiliki atau keinginan pada penerima, dan kata-kata tersebut seringkali digunakan bersamaan dengan simbol dolar "$" sebagai tambahan atau digunakan untuk menunjukkan sejumlah uang. Penawaran gratis atau kesempatan untuk menang seringkali menjadi umpan yang efektif dalam serangan phishing.

Dalam konteks penggunaannya, kata-kata atau kalimat yang terkesan personal atau relevan dengan diri kita seringkali digunakan dalam serangan *spear-phishing*. Melihat frekuensi kemunculan kata-kata tersebut pada Tabel 2, dapat disimpulkan bahwa *spear-phishing* masih sering digunakan oleh para phisher.

Kemudian ada data dari *Anti-Phishing Working Group* (APWG), data ini diambil dari laporan kuarter 4 2023 dan kuarter 1 2024 yang merupakan data terbaru dari APWG. Tercatat dalam laporan APWG kuarter 4 2023 bahwa tahun 2023 merupakan tahun terburuk menurut APWG, bahkan setelah penurunan yang signifikan di pertengahan tahun, jumlah kasus phishing meningkat lagi di akhir tahun. Berikut ini adalah data dari laporan APWG mengenai jumlah serangan phishing.

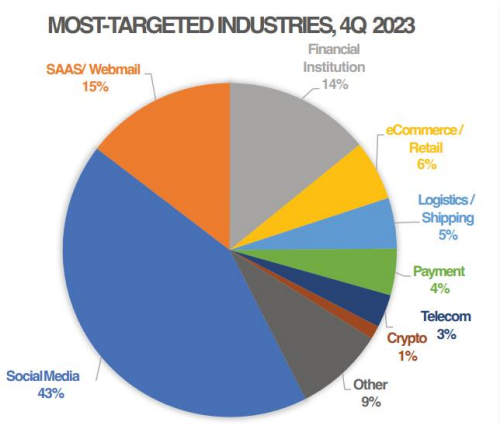
Tabel 3. Jumlah serangan phishing kuarter 4 2023[16]

Oktober	November	Desember
356,538	350,776	370,178
	Jumlah:	1,077,501

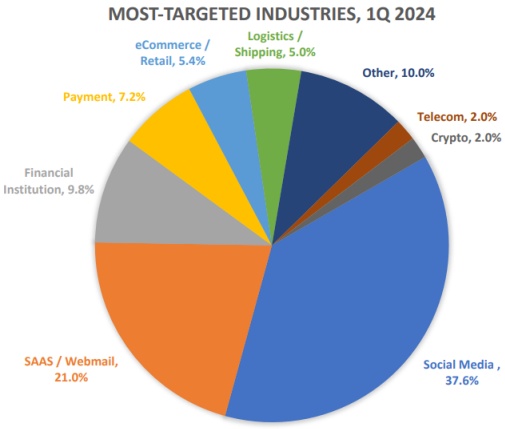
Tabel 4. Jumlah serangan phishing kuarter 1 2024[17]

Januari	Februari	Maret
358,107	314,974	290,913
	Jumlah:	963,994

Dapat dilihat berdasarkan Tabel 3 dan Tabel 4 diatas, bahwa serangan phishing mengalami penurunan dari penghujung tahun 2023 hingga awal tahun 2024. Laporan dari APWG juga mencakup sektor industri yang menjadi target dari serangan phishing.



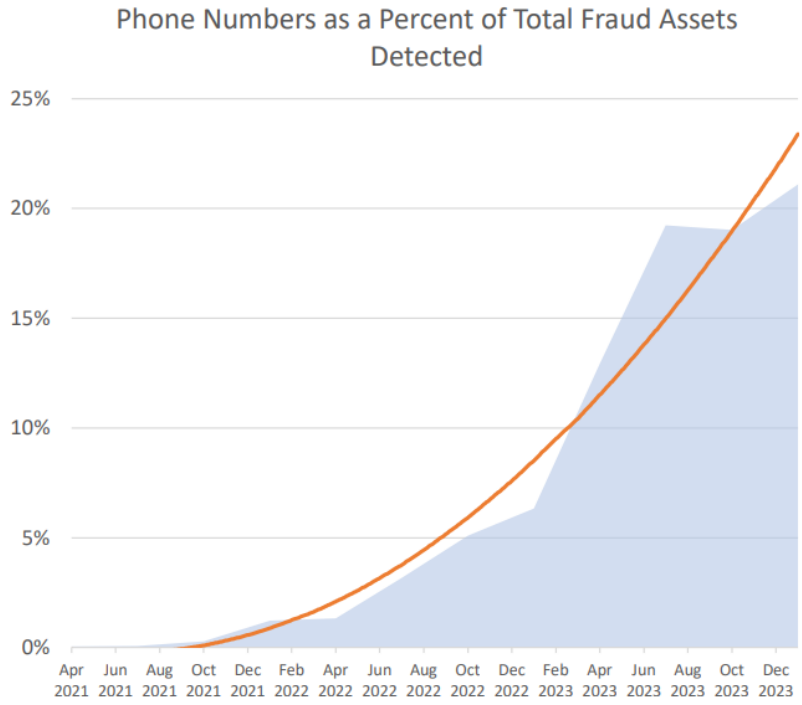
Gambar 2. Target industri kuarter 4 2023, gambar dari *APWG 4Q 2023 Data Report*[16]



Gambar 3. Target industri Januari-Maret 2024, gambar dari *APWG 1Q 2024 Data Report*[17]

Dari Gambar 1 dan Gambar 2 di atas, kita dapat melihat bahwa dari Oktober 2023 hingga Maret 2024, sektor industri yang menjadi target utama serangan phishing adalah Media Sosial, *Webmail*, dan Finansial. Jumlah serangan yang masif terhadap sektor media sosial ini menandakan bahwa metode *deceptive* masih digunakan secara luas, meskipun metode ini tergolong lemah jika targetnya adalah sebuah institusi atau organisasi besar, namun karena banyaknya pengguna media sosial yang berasal dari berbagai kalangan masyarakat, tidak heran metode *deceptive* ini bisa berhasil. Kemudian terjadi peningkatan yang signifikan pada industri *Webmail*, dari 15% menjadi 23%, ini menandakan bahwa terjadi peningkatan yang signifikan terhadap phishing berbasis email. Dengan meninjau kembali hasil analisis Tabel 2, dapat kita katakan bahwa metode *spear-phishing* masih menjadi tren dalam phishing modern.

APWG juga mencatat adanya peningkatan dalam phishing berbasis telepon, di dalamnya mencakup *vishing* (*voice-phishing*), dan *SMiShing* (*SMS-Phishing*).



Gambar 4. Kenaikan jumlah serangan berbasis telepon, gambar dari *APWG 1Q 2024 Data Report*[2]

Berdasarkan Gambar 4 di atas, serangan berbasis telepon mengalami peningkatan yang signifikan dari bulan Februari 2023 hingga Juni 2023, dan setelah mengalami penurunan hingga bulan Oktober 2023, angka ini kemudian naik lagi pada penghujung tahun 2023. Serangan berbasis. Berdasarkan laporan kuarter 1 2024 APWG, serangan phishing berbasis telepon yang umum ditemukan dikenal dengan istilah *hybrid phishing*. *Hybrid phishing* biasanya dilakukan dengan modus tanda terima pembelian atau pembayaran tertentu dengan harga yang sangat tinggi, dan mengharuskan korban untuk menghubungi nomor tertentu dalam waktu singkat untuk menyanggah hal tersebut. Tujuan serangan ini sama dengan kata-kata mendesak pada Tabel 2 yang membuat calon korban panik dan terdesak.

URL juga memainkan peran besar dalam serangan phishing. Dataset dari Prisha Sawhney berisi 176.262 URL phishing yang unik, beserta *domain*-nya dan beberapa komponen penting dari isi *website*-nya. Berikut tingkat kemiripan URL dan *domain* terhadap judul dari *website*-nya. Untuk dataset ini, penulis menerapkan metode analisis tekstual untuk mengidentifikasi komponen-komponen penting yang mungkin menjadi kunci dalam URL, *domain*, dan atribut teks lainnya.

Tabel 5. Persentase kemiripan URL dan *domain* terhadap judul *website*

URL/Domain	Diatas 50%	Dibawah 50%
URL	96251(≈54.1%)	81001(≈45.9%)
Domain	91745(≈52.0%%)	84517(≈47.9%)

Pada Tabel 5 diatas, selisih nilai antara persentase diatas 50% dan dibawah 50% tidaklah besar, ini berarti kemiripan URL dan *domain* terhadap judul tidak bisa dijadikan indikator yang kuat untuk phishing.

Tabel 6. TLD yang digunakan dalam URL

com	org	lainnya
86940(≈49.3%)	15966(≈9.1%)	73356(≈41.6%)

Tabel 6 diatas menunjukkan *Top Level Domain* atau TLD yang digunakan dalam URL phishing dalam data. Dapat dilihat bahwa pada data tersebut, TLD ".com" adalah yang paling sering digunakan, kemudia TLD ".org" yang terkenal akan kredibilitasnya ternyata digunakan sebanyak lebih dari 9% dari total URL, dan sisanya adalah TLD yang biasanya merupakan *Country Code* TLD atau TLD yang menggunakan kode negara seperti ".id", ".uk", ".de", dan sebagainya. Bahkan TLD ".org" yang dikenal secara luas akan kredibilitas dan integritasnya yang tinggi bisa digunakan dalam serangan phishing, begitu juga dengan ".com" yang dikenal secara luas bahkan oleh orang awam yang memiliki pengetahuan minim mengenai URL dan *domain*, sehingga tidak heran jika URL phishing seperti ini bisa berhasil. Serangan phishing yang menggunakan TLD ".com" bisa mencakup sebagian besar jenis, termasuk *deceptive*, *spear*, dan bahkan *whaling*. Sedangkan penggunaan TLD ".org" biasanya untuk jenis serangan dengan target yang lebih tinggi seperti *Business e-Mail Compromise* (BEC), dan *whaling*.

Tidak hanya TLD dan judul yang terlihat meyakinkan, sebagian besar *domain* dan URL tersebut juga menggunakan nama perusahaan yang terlihat resmi, serta tercatat bahwa sekitar 79% URL pada dataset tersebut menggunakan *Hypertext Transfer Protocol Secure* (HTTPS), dan hanya 21% URL yang menggunakan *Hypertext Transfer Protocol* (HTTP). Beberapa URL dan *domain* menggunakan huruf, angka, atau simbol pengganti yang mirip untuk mengelabui penglihatan sekilas dari calon korban, misalnya "https://drive.google.com" diubah menjadi "https://drive.go0gle.com", pada link palsu, huruf "o" diganti dengan angka 0. Bahkan ada penyamaran yang lebih kuat lagi seperti "https://google.com/" diubah menjadi "https://goog1e.com". jika hanya dilihat sekilas, kedua link tersebut akan tampak mirip dan tidak ada bedanya, huruf "l" pada link palsu diganti dengan angka 1 sehingga terlihat identik.

3.4. Contoh Studi Kasus Dari Phishing

Studi Kasus: Phishing pada Layanan Online Banking

Sebuah studi kasus mengungkapkan bagaimana seorang pengguna layanan online banking dari Rabobank menjadi korban serangan phishing. Pengguna menerima telepon dari seseorang yang mengaku sebagai representatif bank tersebut. Dalam percakapan tersebut, pelaku phishing (phisher) meminta pengguna untuk memverifikasi email yang diterima dengan alasan untuk menghindari masalah potensial. Jenis phishing yang digunakan dalam kasus ini adalah *spear-phishing*. *Spear-phishing* adalah bentuk phishing yang menargetkan individu tertentu dengan informasi yang dipersonalisasi. Strategi yang digunakan termasuk *social engineering*, di mana phisher menipu korban untuk meyakini bahwa mereka berkomunikasi dengan entitas yang sah (bank) melalui telepon. Phisher memanfaatkan kepercayaan korban terhadap bank dengan maksud untuk memperoleh informasi sensitif. Mereka sering kali meminta pengguna untuk memberikan kredensial, seperti kode random atau identitas, dengan dalih tertentu, sehingga mereka dapat melakukan transaksi atau tindakan ilegal lainnya.

Akibat kelalaian pengguna dalam mengklarifikasi permintaan tersebut kepada pihak bank, serta kurangnya pengetahuan mengenai aturan perbankan yang melarang pengungkapan informasi sensitif melalui telepon, phisher berhasil mendapatkan akses ke akun pengguna dan melakukan transaksi tanpa sepengetahuan pemilik akun. Tindakan yang menyebabkan korban terjerumus adalah ketidakwaspadaan dan kurangnya klarifikasi terhadap permohonan tersebut kepada pihak bank. Pengguna tidak memverifikasi identitas penelepon dengan pihak bank yang sebenarnya, yang merupakan langkah krusial untuk mencegah phishing.

Sasaran phishing dalam kasus ini adalah nasabah bank, yang dapat berasal dari berbagai lapisan masyarakat, termasuk pemilik bisnis, karyawan, atau bahkan anggota keluarga seperti bibi atau anak, selama mereka memiliki akses ke layanan perbankan online. Namun, seringkali target utamanya adalah individu yang dianggap memiliki pengetahuan yang kurang dalam hal keamanan digital. Penelitian ini juga menyoroti faktor lain yang membuat pengguna rentan terhadap serangan phishing, seperti kebiasaan menggunakan kata sandi yang sama untuk berbagai akun, serta pemilihan kata sandi yang mudah ditebak seperti nama anak, nama hewan peliharaan, atau tanggal ulang tahun. Praktik-praktik ini secara signifikan mempermudah tugas phisher dalam mengakses akun-akun korban.

Berdasarkan beberapa penelitian sebelumnya, telah teridentifikasi empat alasan utama mengapa pengguna menjadi korban phishing:

- Banyaknya email yang diterima meningkatkan peluang penipuan.
- Pengguna cenderung membuka email dari entitas yang mereka kenal.
- Kurangnya pengetahuan mengenai ancaman phishing.
- Kebiasaan penggunaan media, seperti mengecek email setiap pagi tanpa kewaspadaan .

Teknik penipuan phishing seringkali melibatkan penyamaran sebagai entitas sah melalui email atau situs web yang tampak resmi, yang

semakin memperdaya pengguna untuk memberikan informasi sensitif.

Studi kasus ini menunjukkan betapa pentingnya edukasi dan peningkatan kesadaran pengguna terhadap ancaman phishing, serta pentingnya penerapan praktik keamanan yang ketat dalam penggunaan layanan online banking. Kewaspadaan yang kurang diperhatikan oleh korban termasuk tidak memverifikasi identitas penelepon dengan pihak bank, mengabaikan protokol keamanan perbankan seperti tidak mengungkapkan informasi sensitif melalui telepon atau email, dan kurangnya pengetahuan tentang teknik social engineering yang sering digunakan dalam serangan phishing.

Pelaku phishing dapat diambil tindakan sesuai dengan berbagai undang-undang yang berkaitan dengan kejahatan siber. Misalnya, di Indonesia, mereka dapat dituntut berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur berbagai tindak pidana di ranah siber, termasuk phishing. Selain itu, Undang-Undang Perlindungan Data Pribadi juga menjadi landasan hukum yang melindungi data pribadi dari penyalahgunaan. Korban serangan phishing memiliki hak untuk memperoleh ganti rugi, yang mungkin mencakup pengembalian dana yang hilang akibat transaksi yang tidak sah serta kompensasi atas kerugian lain yang timbul akibat pelanggaran keamanan tersebut.

3.4. Investigasi Serangan Phishing

Dengan pendekatan forensik, serangan phishing dapat diinvestigasi dengan melibatkan serangkaian langkah sistematis untuk mengidentifikasi dan menganalisis bukti-bukti digital dan komponen penyerangan yang terkait dengan serangan phishing. Investigasi phishing melibatkan serangkaian tahapan sistematis yang membutuhkan keahlian teknis khusus dan beberapa keahlian non-teknis seperti kemampuan analisis, problem solving, komunikasi, manajemen, dan ketelitian untuk melakukan investigasi secara efektif dan efisien. Berikut adalah tahapan investigasi yang ideal untuk kasus phishing dengan pendekatan forensik:

Pengumpulan Bukti dan Komponen Serangan

Setelah serangan phishing terjadi, kumpulkan bukti relevan seperti email phishing, log sistem, dan informasi jaringan. Identifikasi sumber phishing dengan menganalisis header dan lampiran email, atau link palsu yang dibuka. Pemahaman jaringan komputer dan protokol komunikasi diperlukan untuk melacak aktivitas mencurigakan.

Pemeriksaan Perangkat Korban

Periksa perangkat korban dengan mengisolasi perangkat dari jaringan untuk mencegah penyebaran. Analisis dilakukan pada salinan media penyimpanan untuk menjaga integritas bukti. Deteksi malware menggunakan alat tertentu, dan jika perlu, lakukan reverse engineering untuk memahami cara kerja malware.

Pemulihan dan Mitigasi

Langkah mitigasi meliputi identifikasi infeksi, pemulihan data dari cadangan, dan penggantian kredensial yang terkompromi dengan kata sandi yang kuat. Gunakan Multi Factor Authentication (MFA) untuk meningkatkan keamanan. Setelah itu, monitor aktivitas mencurigakan dengan Intrusion Detection System (IDS), Intrusion Prevention System (IPS), dan Security Information and Event Management (SIEM).

Pembuatan Laporan

Setelah investigasi, buat laporan yang terstruktur mencakup gambaran umum serangan, alat dan metode yang digunakan, serta temuan. Sertakan bukti digital seperti log aktivitas, email phishing, dan URL palsu. Laporan ini dapat dilaporkan ke penegak hukum atau otoritas terkait untuk tindakan lanjut.

4. DISKUSI

Berdasarkan analisis dan studi kasus yang telah dilakukan, ditemukan bahwa serangan phishing sering terjadi melalui beberapa metode: (1) penawaran melalui email dengan metode *deceptive* dan *spear*; (2) *web-phishing* melalui URL yang terlihat resmi; (3) gabungan *Business eMail Compromise* (BEC) dengan *spear* atau *whaling* kepada personil dengan status tinggi dalam perusahaan. Temuan ini didukung oleh penelitian Fauzi dan rekan-rekannya yang menunjukkan bahwa serangan phishing berbasis email adalah salah satu metode serangan yang paling umum digunakan oleh penjahat siber. Sari dan rekan-rekannya juga mengemukakan metode serangan *whaling* yang menargetkan individu dengan kedudukan tinggi dalam perusahaan seperti CEO atau CFO, namun metode ini diperkirakan akan menjadi kurang umum seiring waktu, dikarenakan tingkat personalisasi target dan risiko yang terlalu tinggi.

Serangan phishing sering terjadi karena kurangnya pengetahuan atau faktor psikologis individu. Studi oleh Alabdan juga telah membuktikan hal tersebut. Berikut faktor-faktor penentu kesuksesan serangan phishing menurut penelitit, berdasarkan studi oleh Alabdan.

- Manusia cenderung mematuhi tuntutan dari figur otoritas.
- Prinsip bahwa orang lebih mungkin melakukan sesuatu untuk orang yang mereka sukai (bisa menjadi pendorong bagi calon korban jika phishing tersebut diteruskan oleh orang yang disukai)
- Membuat opsi yang awalnya tidak masuk akal tampak lebih menarik karena lebih disukai dibandingkan dengan pilihan lain.
- Nilai yang dipersepsikan digunakan untuk menggoda seseorang agar melakukan tindakan yang mereka diinginkan.

- Seseorang lebih mungkin mengikuti mayoritas daripada mengambil risiko membuat kesalahan. Ini disebut "Mentalitas Kawanan".

Terakhir, tahapan investigasi serangan phishing penting untuk mengidentifikasi sumber dan pelaku serangan, memungkinkan penegakan hukum dan pencegahan serangan di masa depan. Dengan memahami cara serangan terjadi, sebuah individu atau organisasi dapat memperbaiki kerentanan dalam sistem mereka, memperkuat pertahanan, dan mengurangi risiko serangan di masa depan. Selain itu, hasil investigasi meningkatkan kesadaran dan pelatihan tiap individu, membantu memulihkan data yang dicuri, dan memperkuat kebijakan serta prosedur keamanan. Respon proaktif terhadap serangan juga meningkatkan reputasi dan kepercayaan dari pelanggan dan mitra bisnis.

5. KESIMPULAN

Serangan phishing memiliki dampak yang bervariasi mulai dari yang ringan seperti kebingungan dan waktu yang terbuang, hingga kerugian besar seperti kerugian finansial dan data pribadi yang bocor. Serangan ini seringkali menggunakan pola yang sama seperti email yang mengatasnamakan organisasi atau perusahaan terpercaya, phishing yang ditujukan khusus ke satu individu atau organisasi, atau pesan yang berisi tautan palsu. Metode investigasi phishing dengan pendekatan forensik ditentukan berdasarkan jenis serangan phishing yang terjadi. Metode pemulihan data sederhana dapat dilakukan oleh orang awam, namun untuk kasus yang lebih kompleks, disarankan untuk meminta bantuan profesional. Kualitas serangan phishing ke depannya sangat memungkinkan untuk terjadi perkembangan, mengingat perkembangan teknologi yang pesat juga menjadi faktor yang mempengaruhi serangan phishing. Dengan bantuan teknologi seperti Artificial Intelligence (AI) dan alat untuk memanipulasi suara atau media lainnya, serangan phishing menjadi lebih berbahaya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu dalam pelaksanaan penelitian ini.

DAFTAR PUSTAKA

[1] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science*, vol. 3, pp. 1–23, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[2] P. Sari and T. Sutabri, "Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari," *Jurnal Digital Teknologi Informasi*, vol. 6, no. 1, p. 29, Mar. 2023, doi: 10.32502/digital.v6i1.5620.

[3] H. Ahmadian and A. Sabri, "TEKNIK PENYERANGAN PHISHING PADA SOCIAL ENGINEERING MENGGUNAKAN SET DAN PENCEGAHANNYA," *Djtechno : Journal of Information Technology Research*, vol. 2, no. 1, pp. 13–20, Jul. 2021, ISSN: 2745-375.

[4] A. Ali, S. Khayati, and S. L. Fatmawati, "Perlindungan Hukum Terhadap Data Pribadi Nasabah Debitur Indonesia Legal Protection of Indonesian Debtor Customer Personal Data," *Jurnal Hukum*, vol. 4, pp. 8–16, 2022, doi: 10.54297/surel.v4i1.43.

[5 B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers and Security*, vol. 132. pp. 1–25, 2023. doi: 10.1016/j.cose.2023.103387.

[6] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or Not Phishing? A Survey on the Detection of Phishing Websites," *IEEE Access*, vol. 11, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135.

[7] A. Safi and S. Singh, "A systematic literature review on phishing website detection techniques," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 590–611, Feb. 2023, doi: 10.1016/j.jksuci.2023.01.004.

[8] A. Ozcan, C. Catal, E. Donmez, and B. Senturk, "A hybrid DNN–LSTM model for detecting phishing URLs," *Neural Computing and Applications*, vol. 35, no. 7, pp. 4957–4973, Aug. 2023, doi: 10.1007/s00521-021-06401-z.

[9] P. K. Yeng, M. A. Fauzi, B. Yang, and P. Nimbe, "Investigation into Phishing Risk Behaviour among Healthcare Staff," Information (Switzerland), vol. 13, no. 8, 2022. doi: 10.3390/info13080392.

[10] M. Nadhif Hermanto, "ANALISIS FORENSIC BERBASIS WEB PHISING MENGGUNAKAN METODE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY," *Cipta Cendikia Kotabumi Jurnal informasi dan Komputer*, vol. 11, no. 1, pp. 116–123, 2023, doi: 10.35959/jik.v11i01.311.

[11] A. Al-Subaiey, M. Al-Thani, N. A. Alam, A. Khandakar, S. M. Ashfaq, and U. Zaman, "Novel Interpretable and Robust Web-based AI Platform for Phishing Email Detection," *Cornell University*, pp. 1–19, May 2024, doi: 10.48550/arXiv.2405.11619.

[12] N. Muslim, O. Senjaya, F. Hukum, U. Singaperbangsa, and K. Abstrak, "PERTANGGUNGJAWABAN HUKUM PLATFORM MEDIA SOSIAL TERHADAP KORBAN PHISING MELALUI MASS TAGGING PORNOGRAFI," *Jurnal Ilmu Hukum dan Humaniora*, vol. 9, no. 2, pp. 955–963, 2022, doi: 10.31604/justitia.v9i2.

[13] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems*, vol. 76, no. 1. pp. 139–154, 2021. doi: 10.1007/s11235-020-00733-2.

[14] S. H. Abbas, W. A. K. Naser, and A. A. Kadhim, "Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)," Global Journal of Engineering and Technology Advances, vol. 14, no. 2, 2023. doi: 10.30574/gjeta.2023.14.2.0031.

[15] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, pp. 1–39, 2020, doi: 10.3390/fi12100168.

[16] APWG, "Phishing Activity Trends Report_4th Quarter of 2023," Feb. 2023. [Online]. Available: www.apwg.org.

[17] APWG, "Phishing Activity Trends Report_1st Quarter of 2024," May 2024. [Online]. Available: http://www.apwg.org.