E-ISSN 3026 - 3204
Leuser: Jurnal Hukum Nusantara
Open Access: https://journal.myrepublikcorp.com/index.php/leuser

ANALISIS KEJAHATAN *ONLINE PHISHING* PADA MASYARAKAT

Kelas 4A4[1], Octo Iskandar[2]
Fakultas Hukum, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia[1,2]
e-mail: bhayangkara@mhs.ubharajaya.ac.id[1], octoiskandar19@gmail.com[2]

ABSTRACT

Online Phishing Crimes pose a significant threat to society by exploiting human vulnerabilities to steal sensitive information, leading to financial loss and identity theft. Phishing is a common online fraud technique in which fake emails are created to appear legitimate, with the aim of tricking recipients into divulging sensitive information such as symbols or codes, credit card details, and so on. This form of social engineering exploits both human behavior and technology, with research emphasizing the importance of understanding both aspects in combating phishing attacks. Despite advances in anti-phishing technology, the threat of phishing remains significant in today's digital landscape, requiring continued development to improve prevention measures and protect users from falling victim to these fraudulent schemes. Various anti-phishing techniques, including laws and software solutions, have been enhanced to minimize the risks associated with phishing attacks, highlighting the need for a multi-faceted approach to effectively combat this online security threat. Preventive measures, such as analyzing phishing messages and classifying phishing attacks, are essential to increase user awareness and improve protection systems against these online threats.

KEYWORD:

Cyber Crime, Crime, Phishing

ABSTRAK

Kejahatan *Phishing Online* menimbulkan ancaman signifikan bagi masyarakat dengan mengeksploitasi kerentanan manusia untuk mencuri informasi sensitif, yang menyebabkan kerugian finansial dan pencurian identitas. *Phishing* adalah teknik penipuan *daring* yang lazim di mana *email* palsu dibuat agar tampak sah, dengan tujuan menipu penerima agar membocorkan informasi sensitif seperti isyarat ataupun kode, detail kartu kredit, dan sebagainya. Bentuk rekayasa sosial ini mengeksploitasi perilaku manusia dan teknologi, dengan penelitian yang menekankan pentingnya memahami kedua aspek tersebut dalam memerangi serangan *phishing*. Meskipun ada kemajuan dalam teknologi *anti-phishing*, ancaman phishing tetap signifikan dalam lanskap digital saat ini, sehingga diperlukan pengembangan berkelanjutan untuk meningkatkan langkah-langkah pencegahan dan melindungi pengguna agar tidak menjadi korban skema penipuan tersebut. Berbagai teknik anti-*phishing*, termasuk undang-undang dan solusi perangkat lunak, sehabis ditingkatkan untuk meminimalisir risiko yang berhubungan dengan serangan phishing, menyoroti perlunya pendekatan multi-sisi untuk memerangi ancaman keamanan online ini secara efektif. Tindakan pencegahan, seperti menganalisis pesan *phishing* dan mengklasifikasikan serangan *phishing*, sangat penting untuk meningkatkan kesadaran pengguna dan meningkatkan sistem perlindungan terhadap ancaman *online* ini.

KATA KUNCI

Cyber Crime, Kejahatan, *Phishing*

INFO ARTIKEL

Sejarah Artikel:
Diterima: 25 Juni 2024
Direvisi: 27 Juni 2024
Disetujui: 29 Juni 2024

CORRESPONDING AUTHOR

Kelas 4A4
Universitas Bhayangkara Jakarta Raya
Jakarta
bhayangkara@mhs.ubharajaya.ac.id

PENDAHULUAN

Internet kini menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari. Penggunaan internet mulai berkembang pesat sejak awal tahun 2000-an. Seiring dengan meningkatnya penggunaan internet dalam kehidupan manusia, internet dimanfaatkan dalam berbagai bidang seperti pendidikan, komunikasi, ekonomi, dan lainnya. Namun, perkembangan internet ini dianggap sebagai pedang bermata dua. Di satu sisi, internet membawa kemudahan dalam kehidupan manusia, tetapi di sisi lain, internet menjadi tempat yang rawan untuk tindak kejahatan. Banyak pihak yang menggunakan internet untuk mencari keuntungan pribadi meskipun merugikan orang lain (Wahyuni et al., 2023). Hal ini menyebabkan munculnya kejahatan siber, yang paling umum adalah phishing (Sari & Sutabri, 2023).

Phishing adalah bentuk kejahatan siber di mana pelaku mencoba mendapatkan informasi pribadi seperti kata sandi, nomor kartu kredit, atau data sensitif lainnya dengan cara menipu korbannya (Hayati

& Fata, 2021). Biasanya, ini dilakukan melalui email, pesan teks, atau situs web palsu yang dibuat agar terlihat seperti sumber yang sah (Saputra Gulo et al., 2020). Remaja, yang sering menjadi pengguna aktif internet, merupakan salah satu kelompok yang rentan terhadap serangan ini . Korban phishing dapat mengalami kerugian finansial, pencurian identitas, dan kerusakan mental (Yustitiana, 2021). Kehilangan uang, pencurian data pribadi, dan depresi akibat penipuan adalah konsekuensi serius yang bisa terjadi (Rian Handoko & Tata Sutabri, 2023). Menurut data dari Cybersecurity and Infrastructure Security Agency (CISA), serangan phishing telah meningkat secara signifikan dalam beberapa tahun terakhir (Chiew et al., 2018). Selain itu, laporan dari Anti-Phishing Working Group (APWG) menunjukkan bahwa pada kuartal pertama tahun 2023, terdapat lebih dari 1,2 juta serangan phishing yang terdeteksi di seluruh dunia.

Tujuan penelitian ini adalah untuk menganalisis dan memahami berbagai aspek kejahatan online phishing yang mempengaruhi masyarakat. Penelitian ini bertujuan mengidentifikasi faktor-faktor penyebab terjadinya phishing di kalangan masyarakat serta menjelaskan modus operandi yang digunakan oleh pelaku dalam menjalankan aksinya. Selain itu, penelitian ini juga bertujuan mengukur tingkat pengetahuan dan kesadaran masyarakat mengenai phishing dan cara-cara pencegahannya, serta mengevaluasi dampak kejahatan ini terhadap individu dan masyarakat, termasuk kerugian finansial dan psikologis yang ditimbulkan.

METODE

Metode penelitian hukum yuridis untuk studi tentang "Analisis Kejahatan Online Phishing pada Masyarakat" melibatkan langkah-langkah yang sistematis dalam mengumpulkan dan menganalisis data hukum terkait kejahatan siber ini. Pertama, penelitian akan memulai dengan studi literatur yang mendalam untuk memahami landasan hukum yang mengatur kejahatan phishing, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan lain yang relevan di Indonesia. Selanjutnya, metode ini akan melibatkan analisis mendalam terhadap kasus-kasus hukum yang telah ditangani oleh sistem peradilan terkait dengan kejahatan phishing, untuk mengevaluasi penggunaan hukum dan dampaknya terhadap korban serta pelaku kejahatan. Wawancara dengan ahli hukum yang memiliki keahlian dalam bidang kejahatan siber juga akan dilakukan untuk mendapatkan perspektif yang mendalam mengenai implementasi undang-undang dan peraturan terkait. Hasil dari penelitian ini diharapkan dapat memberikan rekomendasi hukum untuk memperkuat perlindungan terhadap korban, meningkatkan efektivitas penegakan hukum, dan merumuskan strategi pencegahan yang lebih baik dalam menanggulangi kejahatan phishing di Indonesia.

HASIL DAN PEMBAHASAN

Pengertian *Phishing*

Phishing memiliki dampak yang merugikan bagi individu dan masyarakat secara keseluruhan (Gading, 2023). Bagi individu, dampak utamanya adalah kerugian finansial akibat pencurian data kartu kredit atau informasi perbankan (Darmaningrat et al., 2022). Selain itu, pencurian identitas dapat menyebabkan masalah jangka panjang, seperti kerusakan reputasi dan kesulitan mengakses layanan keuangan (Fatimah, 2017). Bagi masyarakat, tingginya insiden phishing dapat mengurangi kepercayaan terhadap transaksi digital dan memperlambat adopsi teknologi baru (Butarbutar, 2023).

Pengguna internet yang kurang waspada menjadi target utama para penjahat cyber dalam melancarkan aksi phishing (Syah, 2023). Hal ini disebabkan oleh beberapa faktor, antara lain kurangnya edukasi dan literasi digital, yang membuat banyak orang tidak mengetahui cara kerja phishing dan bagaimana melindungi diri dari kejahatan ini. Selain itu, ketidakhati-hatian pengguna yang sering tergoda dengan tawaran menarik atau informasi yang tampak kredibel tanpa verifikasi terlebih dahulu, serta teknologi phishing yang semakin canggih, turut meningkatkan risiko menjadi korban (Wijaya & Nurnawati, 2022).

Rendahnya tingkat edukasi masyarakat terhadap keamanan siber juga memperbesar peluang mereka menjadi korban kejahatan siber. Menurut survei yang kami lakukan, dari 30 responden, hanya 20 orang (66,7%) yang pernah mendapatkan pendidikan mengenai keamanan siber, terutama phishing, sementara 10 orang (33,3%) lainnya tidak pernah mendapatkan edukasi tentang keamanan siber atau

bahkan asing dengan istilah tersebut. Data ini menunjukkan bahwa tingkat edukasi tentang keamanan siber masih cukup rendah, terutama di kalangan usia lanjut (Baby Boomer, Gen X) (Fikri et al., 2022).

Phishing merupakan bentuk kejahatan siber yang melibatkan pemalsuan data pada situs web palsu yang tampak mirip dengan situs aslinya, dengan tujuan untuk memperoleh identitas orang lain dan menggunakannya secara ilegal tanpa sepengetahuan pemiliknya (Wahyu Hidayat M et al., 2023). Penipuan ini dilakukan oleh penjahat cyber untuk mendapatkan data pribadi seperti kata sandi, kode, nomor kartu kredit, dan informasi sensitif lainnya melalui penyamaran sebagai individu atau organisasi yang dapat dipercaya (Vadila & Pratama, 2021). Pelaku phishing biasanya mengirim pesan palsu yang tampak seperti email atau teks resmi, sering kali berisi tautan yang mengarahkan korban ke situs web palsu yang meniru situs resmi. Terdapat berbagai modus operandi yang digunakan dalam phishing, termasuk email phishing yang mengirim email tampak resmi dari organisasi terpercaya, situs web phishing yang membuat situs web ilegal menyerupai situs asli seperti bank atau platform media sosial, dan pesan instan phishing yang menyebarkan pesan melalui platform seperti WhatsApp, SMS, atau Telegram, berisi tautan atau lampiran yang mengarahkan ke situs web ilegal atau menanamkan malware (Ardy et al., 2024).

Peran Masyarakat Untuk Mencegah Kejahatan *Phishing Online*

Kemunculan kejahatan online phishing disebabkan oleh kurangnya pengetahuan masyarakat tentang pentingnya menjaga keamanan data mereka (Harahap et al., 2024). Setelah memahami cara kerja phishing, masyarakat dapat menghindari ancaman ini dengan menerapkan beberapa langkah pencegahan. Pertama, mereka perlu berhati-hati dan teliti terhadap email, situs web, dan pesan singkat yang tidak dikenal. Kedua, penting untuk memverifikasi alamat email dan situs web agar sesuai dengan alamat resmi organisasi terkait. Ketiga, penggunaan kata sandi yang kuat dan unik untuk setiap akun sangat dianjurkan. Keempat, mengaktifkan autentikasi dua faktor dapat menambahkan lapisan keamanan ekstra. Kelima, memasang perangkat lunak antivirus dan anti-malware membantu mendeteksi dan mencegah malware. Terakhir, melaporkan aktivitas phishing kepada pihak berwenang seperti Badan Siber dan Sandi Negara (BSSN) juga sangat penting (Mokobombang et al., 2023).

Mempelajari tentang phishing dan berbagi pengetahuan ini dengan teman dan keluarga sangatlah esensial untuk melindungi mereka. Dengan memahami keamanan siber, Anda dapat membantu orang-orang terdekat memahami risiko dan strategi phishing yang umum digunakan. Di Indonesia, pelanggaran siber termasuk phishing telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), sehingga jika mengalami hal tersebut, masyarakat dapat melaporkannya kepada pihak berwenang yang dapat menindaklanjuti sesuai dengan undang-undang yang berlaku (Caniago & Sutabri, 2023).

Sumber Ancaman-Ancaman Kejahatan *Phishing Online*

Ancaman kejahatan phishing online sering muncul ketika masyarakat mengalami perubahan akibat perkembangan teknologi (Hariyono & Simangunsong, 2023). Perkembangan teknologi informasi dan telekomunikasi memiliki dampak besar bagi masyarakat, membawa efek positif dan negatif terhadap perkembangan manusia dan peradabannya. Salah satu dampak negatifnya adalah peningkatan cybercrime, termasuk phishing (Tabrani et al., 2024). Kejahatan phishing yang dilakukan secara online atau elektronik dapat menyebabkan kerugian bagi orang lain dan dilarang oleh undang-undang. Saat ini, media sosial sering dimanfaatkan oleh pihak-pihak tidak bertanggung jawab untuk melakukan phishing online. Modus operandi pelaku phishing melibatkan berbagai media yang terhubung ke internet, seperti email, SMS, dan situs web. Mereka sering menawarkan hadiah kepada target dan memberikan tautan ke situs web palsu. Ketika seseorang mengklik tautan tersebut atau memasukkan data pribadi, datanya akan diretas (Ansyafa et al., 2024).

Phishing adalah kegiatan di mana seseorang berusaha mendapatkan informasi rahasia milik orang lain dengan menggunakan email dan situs web ilegal yang menyerupai situs resmi (Dm et al., 2022). Penting bagi masyarakat untuk memahami bahaya phishing online yang sering terjadi. Misalnya, serangan melalui email meminta korban mengubah informasi melalui tautan yang dikirim, sementara situs web palsu mendesak pengguna untuk mengisi informasi rahasia yang kemudian digunakan untuk pencurian identitas (Permana et al., 2023). Selain itu, serangan malware melibatkan pengiriman file

yang diklaim sebagai penetralisir malware kepada karyawan, yang jika diunduh akan menanamkan malware di komputer (Ramadhan & Nurnawati, 2022). Peran serta masyarakat sangat penting dalam memberantas kejahatan phishing online, dan kerjasama yang baik antara masyarakat dan aparat penegak hukum akan memudahkan pihak kepolisian dalam mengungkap dan menangkap pelaku phishing online (Aziz et al., 2024).

KESIMPULAN

Phishing adalah bentuk kejahatan siber ketika pelaku berupaya memperoleh informasi pribadi para korban seperti kata sandi, nomor kartu kredit, atau data dan kode sensitif lainnya dengan cara menipu korbannya. Umumnya, ini dilangsungkan lewat email, pesan teks, atau situs web ilegal yang modif agar kelihatan seperti situs web yang sah dan resmi. Tujuannya untuk memiliki identitas orang lain atau para korban dan dipakai secara ilegal tanpa ketahuan oleh pemilik asli identitas tersebut. Dalam hal ini jelas saja korban *phishing* mengalami kerugian finansial, pencurian identitas, dan kerusakan mental. Kehilangan uang, data pribadi dicuri, dan depresi merupakan akibat yang timbul dari penipuan *phising* tersebut, dan hal itu merupakan konsekuensi serius yang diterima oleh para korban kejahatan *phising.*

REFERENSI

Ansyafa, K. Z., Fajarudin, M., Fadhil, M., & Neyman, S. N. (2024). Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit. *Journal of Internet and Software Engineering*, *1*(4), 10–10. https://doi.org/10.47134/pjise.v1i4.2641

Ardy, L. A. F., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial. *Journal of Internet and Software Engineering*, *1*(4), 11–11. https://doi.org/10.47134/pjise.v1i4.2753

Aziz, M. I. A., N.b, M. R. A., Alauddin, M. F., & Neyman, S. N. (2024). Simulasi Dan Upaya Edukasi Keamanan Siber Menggunakan Situs Web Phishing. *TEKTONIK : Jurnal Ilmu Teknik*, *1*(4), Article 4. https://doi.org/10.62017/tektonik.v1i4.1497

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, *2*(2). https://scholarhub.ui.ac.id/telj/vol2/iss2/3

Caniago, K., & Sutabri, T. (2023). Tindak Kejahatan Phising Di Sektor Pelayan Di Universitas Bina Insan Lubuklinggau. *Jurasik (Jurnal Riset Sistem Informasi Dan Teknik Informatika)*, *8*(1), Article 1. https://doi.org/10.30645/jurasik.v8i1.548

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Darmaningrat, E. W. T., Ali, A. H. N., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat Tentang Keamanan Informasi. *Sewagati*, *6*(2), Article 2. https://doi.org/10.12962/j26139960.v6i2.92

Dm, M. Y., Addermi, A., & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan Dan Konseling (JPDK)*, *4*(5), 8018–8023. https://doi.org/10.31004/jpdk.v4i5.7977

Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *JoEICT (Journal of Education And ICT)*, *1*(1), Article 1. https://doi.org/10.29100/.v1i1.69

Fikri, A. M., Pertiwibowo, B., Fachrureza, F., Fahri, M. I., & Setyorini, R. I. (2022). Edukasi Kepada Masyarakat Terkait Cara Menghindari Phishing Melalui Pengadaan Webinar. *JPPM (Jurnal Pengabdian Dan Pemberdayaan Masyarakat)*, *6*(1), 113. https://doi.org/10.30595/jppm.v6i1.7543

Gading, M. (2023). Bahaya Phising Di Kalangan Remaja Melek Internet Kepada Siswa/I SMA Pattimura Jakarta Selatan. *Jurnal Pengabdian Masyarakat Mandira Cendikia*, *2*(11), 88–99.

Harahap, H. S., Rahman, A. A., Suraswati, I., & Neyman, S. N. (2024). Memahami Cara Kerja Phishing menggunakan Tools pada Kali Linux. *Journal of Internet and Software Engineering*, *1*(2), 11–11.

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), Article 1. https://doi.org/10.53363/bureau.v3i1.191

Hayati, M., & Fata, D. (2021). Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising. *Djtechno: Jurnal Teknologi Informasi*, *2*(1), Article 1. https://doi.org/10.46576/djtechno.v2i1.1252

Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital. *Jurnal Hukum dan HAM Wara Sains*, *2*(06), Article 06. https://doi.org/10.58812/jhhws.v2i6.447

Permana, I. S., Sampurno, C. B. K., & Ramadhini, R. P. (2023). Edukasi Keamanan Digital Menggunakan Aplikasi Getcontact Pada Masyarakat Desa Panongan Lor, Cirebon. *Perwira Journal of Community Development*, *3*(2), 29–34. https://doi.org/10.54199/pjcd.v3i2.196

Ramadhan, I. H., & Nurnawati, E. K. (2022). Analisis Ancaman Phishing Dalam Layanan E-Commerce. *PROSIDING SNAST*, E31-41. https://doi.org/10.34151/prosidingsnast.v8i1.4169

Rian Handoko, R. H., & Tata Sutabri, T. S. (2023). Analisamachine Learningdengan Algoritma Multi-Layer Perceptronuntuk Penanganan Kejahatan Phishing. *JINTEKS (Jurnal Informatika Teknologi Dan Sains)*, *5*(1), 13–17.

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), Article 2.

Sari, P., & Sutabri, T. (2023). Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari. *Jurnal Digital Teknologi Informasi*, *6*(1), Article 1. https://doi.org/10.32502/digital.v6i1.5620

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, *2*(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594

Tabrani, S., Safitri, V., P, P. A. N., & Hosnah, A. U. (2024). Kejahatan Phishing Ditinjau Dari Perspektif Hukum Dan Kejahatan Siber. *Civilia: Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, *3*(1), Article 1. https://doi.org/10.572349/civilia.v3i1.1609

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan terhadap Ancaman Phishing. *AUTOMATA*, *2*(2), Article 2. https://journal.uii.ac.id/AUTOMATA/article/view/19512

Wahyu Hidayat M, Hartini Ramli, Ikhram, P. M. B., Sidrayanti, Ridhawi, A. R., Mukhtar, N. A., & Renaldy Junedy. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. *Vokatek : Jurnal Pengabdian Masyarakat*, *1*(1), 28–33. https://doi.org/10.61255/vokatekjpm.v1i1.29

Wahyuni, N. K. A. T., Cahayani, P. P., Wicaksana, I. G. N. Y., & Wijayanti, I. A. K. B. (2023). Analisis Kerentanan Kejahatan Online Phising Menggunakan Tools Zphisher, Shellphish Dan Whphisher: Phising. *Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*, *3*(1), 23–31. https://doi.org/10.55606/teknik.v3i1.915

Wijaya, L., & Nurnawati, E. K. (2022). Analisis Kesadaran Mahasiswa Yogyakarta Tentang Phishing Pada Online Banking. *Jurnal Dinamika Informatika*, *11*(2), Article 2.

Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum. *Jurnal Hukum Visio Justisia*, *1*(1), 98–126.