Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 4, 2026
DOI: https://doi.org/10.61104/alz.v4i4.6507

Kajian Kriminologi Kontemporer Terhadap Praktik Phishing Melalui Tautan Digital Palsu

Muhammad Ardan Aldika Rahmat Akbar[1], Erna Dewi[2], Fristia Berdian Tamza[3]
Program Studi Ilmu Hukum, Universitas Lampung, Indonesia[1-3]
Email Korespondensi: aldikaardan@gmail.com, erna.dewi@fh.unila.ac.id, fristia.berdia@fh.unila.ac.id

Article received: 05 Mei 2026, Review process: 12 Mei 2026
Article Accepted : 29 Mei 2026, Article published: 19 Juni 2026

ABSTRACT
The development of digital technology has transformed criminal patterns from conventional crimes into cyber-based crimes, one of which is phishing through fake digital links. This practice uses social engineering techniques to illegally obtain victims' personal data by directing them to fraudulent websites that resemble official platforms. This study aims to analyze phishing as a form of contemporary crime, identify the factors contributing to its occurrence, and examine prevention and countermeasure efforts. This research employs a normative legal research method with statutory and conceptual approaches. Data were collected through library research and analyzed descriptively using a qualitative approach. The findings show that the rise of phishing practices is influenced by low digital literacy, high dependence on digital services, and weak awareness of personal data security. From the perspective of contemporary criminology, phishing represents a modern form of crime that is anonymous, systematic, and difficult to detect. Prevention efforts require strengthening digital literacy, improving technological security systems, and implementing adaptive law enforcement against cybercrime developments.
Keywords: *Phishing, Contemporary Criminology, Cybercrime, Fake Digital Links, Personal Data Protection, Digital Literacy.*

ABSTRAK
Perkembangan teknologi digital telah mendorong perubahan pola kejahatan dari konvensional menjadi kejahatan berbasis siber, salah satunya phishing melalui tautan digital palsu. Praktik ini memanfaatkan rekayasa sosial untuk memperoleh data pribadi korban secara ilegal dengan cara mengarahkan korban pada laman tiruan yang menyerupai situs resmi. Penelitian ini bertujuan untuk menganalisis phishing sebagai bentuk kriminalitas kontemporer, mengidentifikasi faktor penyebab terjadinya phishing, serta mengkaji upaya pencegahan dan penanggulangannya. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan dan konseptual. Data diperoleh melalui studi kepustakaan dan dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa meningkatnya praktik phishing dipengaruhi oleh rendahnya literasi digital masyarakat, tingginya ketergantungan terhadap layanan digital, dan lemahnya kesadaran terhadap keamanan data pribadi. Dalam perspektif kriminologi kontemporer, phishing merupakan bentuk kriminalitas modern yang anonim, sistematis, dan sulit dideteksi. Pencegahan dapat dilakukan melalui penguatan literasi digital, peningkatan keamanan sistem teknologi, dan penegakan hukum yang adaptif terhadap perkembangan kejahatan siber.
Kata Kunci: *Phishing, Kriminologi Kontemporer, Kejahatan Siber, Tautan Digital Palsu, Perlindungan Data Pribadi, Literasi Digital*

PENDAHULUAN

Perkembangan teknologi informasi di era digital telah membawa perubahan besar dalam berbagai aspek kehidupan masyarakat. Transformasi menuju sistem serba digital memberikan kemudahan dan kepraktisan dalam menjalankan berbagai aktivitas, seperti berkomunikasi, bertransaksi, hingga mengakses berbagai layanan publik maupun pribadi secara daring. Kondisi ini membuat masyarakat semakin nyaman dan percaya dalam memanfaatkan layanan digital, termasuk dalam aktivitas keuangan yang sebelumnya dianggap memiliki risiko tinggi. Namun, kemudahan tersebut juga menuntut adanya kemampuan dalam menjaga keamanan digital, sebab rendahnya kewaspadaan pengguna dapat membuka peluang terjadinya berbagai bentuk kejahatan siber (Devi Anjheli, 2024).

Meningkatnya ketergantungan masyarakat terhadap layanan digital sejalan dengan meningkatnya ancaman kejahatan berbasis teknologi. Salah satu bentuk kejahatan siber yang paling sering terjadi dan menjadi perhatian global adalah Phishing. Phishing merupakan praktik penipuan digital yang dilakukan dengan cara memanipulasi korban agar memberikan data pribadi atau informasi penting melalui tautan digital palsu yang menyerupai situs resmi suatu lembaga, platform, atau layanan tertentu. Data yang diperoleh pelaku biasanya berupa identitas pribadi, username, password, kode OTP, hingga informasi perbankan yang kemudian disalahgunakan untuk kepentingan illegal (Maharlina D.P., 2024).

Penipuan digital sendiri merupakan salah satu bentuk kriminalitas siber yang banyak dibahas dalam kajian keamanan digital dan literasi digital. Istilah ini mencakup berbagai bentuk penipuan yang memanfaatkan perangkat komunikasi dan media digital sebagai sarana utama dalam menjalankan aksi kejahatan. Tingginya tingkat akses internet serta ketergantungan masyarakat terhadap layanan digital menyebabkan peluang terjadinya penipuan digital semakin besar. Salah satu modus yang banyak beredar di masyarakat adalah phishing melalui tautan digital palsu yang umumnya disebarkan melalui surat elektronik, pesan singkat, maupun aplikasi media sosial seperti WhatsApp, Telegram, dan Facebook.

Maraknya praktik phishing menunjukkan adanya perubahan pola kriminalitas dari kejahatan konvensional menuju kejahatan modern berbasis digital. Dalam perspektif kriminologi kontemporer, perkembangan teknologi tidak hanya menghadirkan inovasi positif, tetapi juga menciptakan ruang baru bagi pelaku kejahatan untuk menjalankan aksinya secara lebih sistematis, anonim, dan sulit terdeteksi. Pelaku memanfaatkan rendahnya literasi digital masyarakat serta minimnya kesadaran terhadap keamanan siber sebagai celah untuk memperoleh keuntungan secara ilegal. Phishing merupakan salah satu bentuk penipuan digital yang dilakukan dengan cara memancing korban agar secara sukarela memberikan informasi pribadi melalui tautan atau situs palsu yang dibuat menyerupai layanan resmi (Afifah Sahfitri & Rosmalinda, 2024).

Praktik ini umumnya memanfaatkan rekayasa sosial untuk membangun kepercayaan korban, sehingga tanpa sadar korban memasukkan data penting seperti identitas pribadi, username, kata sandi, kode verifikasi, hingga informasi keuangan. Dalam perspektif kriminologi kontemporer, phishing menunjukkan adanya pergeseran pola kejahatan dari bentuk konvensional menuju kejahatan

modern berbasis teknologi. Perkembangan teknologi digital telah menciptakan ruang baru bagi pelaku untuk menjalankan aksinya secara anonim, terstruktur, dan sulit terdeteksi. Kondisi tersebut memperlihatkan bahwa kemajuan teknologi tidak hanya menghadirkan manfaat, tetapi juga melahirkan peluang baru bagi berkembangnya tindak kriminal yang semakin kompleks. Maraknya praktik phishing menunjukkan adanya perubahan pola kriminalitas dari kejahatan konvensional menuju bentuk kejahatan modern berbasis digital yang semakin kompleks. Jika pada masa lalu tindak penipuan umumnya dilakukan melalui interaksi langsung antara pelaku dan korban, maka saat ini pelaku dapat menjalankan aksinya secara jarak jauh dengan memanfaatkan teknologi internet sebagai sarana utama. Dalam perspektif kriminologi kontemporer, kondisi ini menunjukkan bahwa perkembangan teknologi tidak hanya menghasilkan inovasi yang memberikan manfaat bagi kehidupan masyarakat, tetapi juga menciptakan ruang baru yang memungkinkan munculnya bentuk-bentuk kriminalitas yang lebih terorganisir, sistematis, anonim, dan sulit dideteksi oleh aparat penegak hukum.

Kemudahan akses terhadap teknologi digital, tingginya intensitas penggunaan internet, serta rendahnya tingkat literasi digital masyarakat menjadi. faktor utama yang mendorong meningkatnya praktik phishing. Pelaku kejahatan memanfaatkan minimnya pengetahuan masyarakat terkait keamanan siber, seperti kurangnya kemampuan membedakan tautan asli dan palsu, kebiasaan mengakses tautan tanpa verifikasi, serta rendahnya kesadaran dalam menjaga kerahasiaan data pribadi. Situasi ini memberikan peluang besar bagi pelaku untuk menjalankan aksinya secara efektif dengan risiko yang relatif kecil untuk terdeteksi.

Dampak yang ditimbulkan oleh praktik phishing tidak hanya terbatas pada kerugian materiil akibat hilangnya dana atau pencurian informasi pribadi, tetapi juga dapat menimbulkan dampak psikologis yang cukup serius bagi korban. Korban sering kali mengalami rasa takut, kecemasan, hilangnya rasa aman dalam menggunakan layanan digital, hingga menurunnya tingkat kepercayaan terhadap sistem teknologi yang selama ini digunakan dalam kehidupan sehari-hari. Dalam jangka panjang, kondisi tersebut dapat memengaruhi kenyamanan masyarakat dalam beradaptasi dengan perkembangan teknologi digital yang terus berkembang. Fenomena ini menunjukkan bahwa phishing merupakan salah satu bentuk kriminalitas kontemporer yang memerlukan perhatian serius dari berbagai pihak. Penanganannya tidak cukup hanya melalui pendekatan hukum, tetapi juga memerlukan peningkatan literasi digital masyarakat, penguatan sistem keamanan siber, serta kerja sama antara pemerintah, penyedia layanan digital, dan masyarakat dalam menciptakan ruang digital yang aman. Berdasarkan latar belakang tersebut, kajian ini bertujuan untuk menganalisis praktik phishing melalui tautan digital palsu dalam perspektif kriminologi kontemporer, mengidentifikasi faktor-faktor yang mendorong terjadinya kejahatan tersebut, serta mengkaji berbagai upaya pencegahan yang dapat dilakukan guna meminimalkan risiko kejahatan digital ditengah pesatnya perkembangan teknologi informasi.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif atau yuridis normatif. Metode penelitian hukum normatif merupakan penelitian yang menempatkan hukum sebagai suatu sistem norma yang dikaji melalui bahan pustaka atau data sekunder, meliputi peraturan perundang-undangan, literatur ilmiah, doktrin para ahli, jurnal hukum, serta berbagai sumber hukum lain yang relevan. Penelitian hukum normatif merupakan penelitian yang berfokus pada kaidah, asas, teori, dan doktrin hukum guna menemukan jawaban atas persoalan hukum melalui pendekatan konseptual dan analisis terhadap norma hukum yang berlaku (Nurhayati, Ifrani, & Said., 2021). Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai ketentuan hukum yang berkaitan dengan tindak pidana siber, khususnya praktik Phishing melalui tautan digital palsu, serta regulasi terkait perlindungan data pribadi di Indonesia. Sementara itu, pendekatan konseptual digunakan untuk memahami teori-teori kriminologi kontemporer yang relevan dalam menganalisis fenomena phishing sebagai bentuk kejahatan modern berbasis teknologi (Tan, 2021).

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer mencakup berbagai peraturan perundang-undangan yang mengatur tindak pidana siber serta perlindungan data pribadi. Adapun bahan hukum sekunder meliputi jurnal ilmiah, buku, hasil penelitian terdahulu, artikel akademik, serta doktrin para ahli yang berkaitan dengan penelitian hukum normatif dan perkembangan kejahatan siber. Penggunaan bahan hukum sekunder bertujuan untuk memperkuat landasan teoritis sekaligus memperkaya analisis terhadap objek penelitian secara komprehensif (Benuf & Azhar, 2020). Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), yaitu dengan cara menginventarisasi, mengidentifikasi, dan menelaah berbagai referensi yang memiliki keterkaitan dengan objek penelitian. Seluruh bahan hukum yang telah terkumpul kemudian dianalisis menggunakan teknik analisis kualitatif dengan metode deskriptif-analitis. Analisis ini dilakukan dengan menguraikan berbagai fakta hukum mengenai praktik phishing melalui tautan digital palsu, kemudian menghubungkannya dengan teori kriminologi kontemporer guna memperoleh pemahaman yang mendalam terkait faktor penyebab, pola pelaksanaan kejahatan, serta upaya pencegahannya (Wiraguna, 2024).

HASIL DAN PEMBAHASAN

Konsep dan Karakteristik Praktik Phishing melalui Tautan Digital Palsu

Phishing merupakan salah satu bentuk kejahatan siber yang dilakukan dengan cara menipu pengguna internet agar secara tidak sadar menyerahkan informasi penting melalui media digital palsu. Informasi yang menjadi sasaran umumnya berupa identitas pribadi, kata sandi, kode verifikasi, data rekening, maupun informasi finansial lainnya. Bentuk penipuan ini biasanya dilakukan dengan membuat tampilan digital yang menyerupai situs resmi suatu institusi

sehingga korban percaya bahwa tautan tersebut berasal dari sumber yang sah (Latifahi, Mawardi, & Wardhana, 2022).

Phishing tidak hanya dilakukan melalui surat elektronik, tetapi juga menyebar melalui berbagai platform komunikasi digital seperti pesan singkat, media sosial, hingga aplikasi percakapan instan seperti WhatsApp dan Telegram. Pelaku biasanya menyisipkan tautan palsu dengan narasi tertentu, misalnya pemberitahuan akun bermasalah, hadiah undian, pembaruan data rekening, atau file undangan digital. Strategi tersebut dirancang untuk menciptakan kepanikan atau rasa penasaran sehingga korban terdorong untuk segera mengakses tautan tanpa melakukan verifikasi terlebih dahulu (Syah, 2023). Secara konseptual, phishing bekerja dengan memanfaatkan teknik social engineering atau rekayasa sosial, yaitu pendekatan manipulatif yang memanfaatkan sisi psikologis korban. Pelaku berupaya membangun kepercayaan dengan menggunakan identitas visual yang menyerupai institusi resmi, bahasa formal, serta penyampaian informasi yang tampak mendesak. Ketika korban membuka tautan tersebut, korban diarahkan menuju laman palsu yang menyerupai halaman asli dan diminta memasukkan data pribadi. Data tersebut kemudian direkam oleh pelaku untuk digunakan dalam tindakan kriminal lanjutan seperti pembobolan akun, pengurasan saldo, atau pencurian identitas digital (Yurita, Ramadhan, & Candra, 2023).

Karakteristik utama phishing melalui tautan digital palsu dapat dikenali melalui beberapa ciri. Pertama, tautan yang digunakan umumnya memiliki alamat domain yang menyerupai situs resmi, namun terdapat perbedaan kecil seperti tambahan karakter, perubahan ejaan, atau penggunaan ekstensi yang tidak lazim. Kedua, pesan yang dikirim sering kali memuat unsur ancaman atau desakan agar korban segera bertindak. Ketiga, terdapat permintaan informasi pribadi secara langsung yang sebenarnya tidak pernah diminta oleh institusi resmi melalui media digital. Keempat, tampilan laman palsu sering kali meniru identitas visual lembaga tertentu secara detail untuk memperkuat kesan autentik (Fatiha, 2024). Maraknya praktik phishing menunjukkan bahwa kejahatan digital terus berkembang mengikuti perubahan pola interaksi masyarakat modern. Tingginya aktivitas digital masyarakat menjadikan ruang siber sebagai target empuk bagi pelaku. Rendahnya literasi keamanan digital memperbesar peluang keberhasilan tindakan phishing karena banyak pengguna belum memahami cara memverifikasi tautan maupun mengenali indikasi manipulasi digital. Kondisi ini menegaskan bahwa phishing merupakan bentuk kriminalitas kontemporer yang berkembang seiring kemajuan teknologi informasi dan membutuhkan perhatian serius dalam upaya pencegahan maupun penanganannya (Anjheli, 2024).

Phishing sebagai Bentuk Kriminalitas Kontemporer dalam Perspektif Kriminologi. Perkembangan teknologi digital telah mengubah banyak aspek kehidupan masyarakat, termasuk dalam pola terjadinya tindak kejahatan. Jika sebelumnya tindakan kriminal lebih sering dilakukan secara langsung dengan mempertemukan pelaku dan korban pada satu tempat, saat ini kejahatan dapat dilakukan melalui media digital tanpa adanya kontak fisik. Salah satu bentuk kejahatan yang berkembang seiring kemajuan teknologi tersebut adalah Phishing. Modus ini dilakukan dengan memanfaatkan tautan digital palsu untuk

memperoleh informasi pribadi milik korban secara tidak sah. Kehadiran phishing memperlihatkan bahwa perkembangan teknologi telah memunculkan pola kriminalitas baru yang menyesuaikan dengan perubahan perilaku masyarakat modern (Ramadhan, 2022). Dalam kajian kriminologi kontemporer, munculnya phishing menunjukkan adanya pergeseran bentuk kejahatan dari pola konvensional menuju pola digital. Perubahan ini terjadi karena ruang digital menyediakan banyak peluang bagi pelaku untuk menjalankan aksi kejahatan dengan cara yang lebih mudah dan sulit terdeteksi. Berbeda dengan penipuan tradisional yang biasanya membutuhkan interaksi langsung, phishing memungkinkan pelaku menargetkan banyak korban secara bersamaan hanya melalui perangkat digital. Situasi ini menunjukkan bahwa perkembangan teknologi selain memberikan manfaat, juga membuka ruang baru bagi lahirnya berbagai bentuk kejahatan modern (Benuf & Azhar, 2021).

Teori aktivitas rutin (Routine Activity Theory), menjelaskan bahwa praktik phishing dapat terjadi karena adanya pertemuan antara pelaku yang memiliki niat melakukan kejahatan, target yang rentan, serta lemahnya pengawasan digital. Pelaku memanfaatkan rendahnya kemampuan sebagian masyarakat dalam mengenali ancaman siber, seperti sulit membedakan tautan asli dan tautan palsu. Di sisi lain, minimnya kehati-hatian pengguna saat menerima pesan digital juga menjadi peluang bagi pelaku untuk menjalankan aksinya dengan lebih mudah. Kondisi ini menunjukkan bahwa keberhasilan phishing tidak hanya dipengaruhi oleh kecanggihan pelaku, tetapi juga oleh lemahnya perlindungan dan kesadaran keamanan digital pengguna (Nurhayati, Ifrani, & Said, 2021). Karakteristik lain yang menjadikan phishing sebagai bentuk kriminalitas kontemporer adalah sifatnya yang anonim dan tidak terbatas wilayah. Pelaku dapat menyembunyikan identitas melalui akun palsu, penggunaan domain tiruan, maupun sistem digital tertentu yang menyulitkan proses pelacakan. Selain itu, kejahatan ini dapat dilakukan lintas daerah bahkan lintas negara tanpa hambatan ruang dan waktu. Hal tersebut menjadi tantangan tersendiri bagi aparat penegak hukum karena penanganannya membutuhkan kemampuan teknologi yang memadai serta koordinasi hukum yang lebih luas (Wijaya, 2023).

Meningkatnya penggunaan layanan digital oleh masyarakat juga menjadi salah satu faktor yang memperbesar risiko terjadinya phishing. Saat ini berbagai aktivitas seperti transaksi keuangan, belanja daring, hingga pengelolaan data pribadi dilakukan melalui internet. Ketergantungan yang tinggi terhadap sistem digital ini menciptakan peluang bagi pelaku untuk memanfaatkan kelengahan pengguna. Banyak masyarakat yang masih kurang memahami pentingnya menjaga kerahasiaan data pribadi dan melakukan verifikasi terhadap tautan yang diterima, sehingga menjadi sasaran empuk bagi pelaku phishing (Fauzi, 2024). Phishing dapat dipahami sebagai bentuk kriminalitas kontemporer yang lahir dari perubahan sosial akibat digitalisasi. Penanganan terhadap kejahatan ini tidak cukup hanya melalui pendekatan hukum semata, tetapi juga perlu dibarengi dengan peningkatan literasi digital masyarakat serta penguatan sistem keamanan teknologi. Dengan langkah tersebut, potensi berkembangnya phishing sebagai ancaman kejahatan modern dapat diminimalkan secara lebih efektif.

Analisis Kasus Praktik Phishing melalui Tautan Digital Palsu di Indonesia

Praktik phishing di Indonesia terus berkembang seiring meningkatnya aktivitas masyarakat dalam memanfaatkan layanan digital, terutama pada sektor perbankan, transaksi elektronik, dan komunikasi daring. Salah satu pola yang paling sering ditemukan adalah penyebaran tautan digital palsu yang dibuat menyerupai situs resmi suatu lembaga atau platform tertentu. Pelaku umumnya menyebarkan tautan tersebut melalui pesan singkat, surat elektronik, maupun aplikasi percakapan digital seperti WhatsApp dan Telegram dengan menyisipkan pesan yang dirancang untuk menimbulkan rasa mendesak atau kepanikan pada korban. Modus ini mendorong korban untuk segera membuka tautan tanpa melakukan pemeriksaan lebih lanjut terhadap keasliannya (Salsabila, 2025).

Salah satu contoh kasus yang marak terjadi di Indonesia adalah penyebaran tautan palsu berkedok verifikasi akun perbankan atau pembaruan data layanan digital. Dalam praktiknya, korban menerima pesan yang mengatasnamakan institusi resmi dan diarahkan untuk mengakses tautan tertentu guna melakukan pembaruan data. Sekilas tampilan laman tersebut dibuat sangat mirip dengan halaman asli, baik dari segi logo, tata letak, maupun warna visual, sehingga sulit dibedakan oleh pengguna awam. Ketika korban memasukkan data seperti nomor rekening, kata sandi, PIN, maupun kode OTP, seluruh informasi tersebut secara otomatis terekam dan dapat diakses oleh pelaku untuk melakukan tindakan lanjutan seperti pengambilalihan akun atau pengurasan saldo korban.

Gambar 1. Contoh Pishing

Praktik phishing dapat terjadi karena adanya pertemuan antara pelaku yang memiliki motivasi ekonomi, target yang rentan akibat rendahnya literasi keamanan digital, serta lemahnya perlindungan teknologi maupun kewaspadaan pengguna. Tingginya penggunaan layanan digital di Indonesia menjadi peluang besar bagi pelaku untuk memperluas target secara masif. Selain itu, rendahnya kebiasaan masyarakat dalam memverifikasi alamat tautan dan memahami ciri situs palsu semakin meningkatkan kemungkinan keberhasilan serangan ini. Dampak yang ditimbulkan dari praktik phishing tidak hanya berupa kerugian finansial, tetapi juga menimbulkan gangguan psikologis berupa rasa cemas, takut, dan menurunnya kepercayaan masyarakat terhadap sistem digital. Banyak korban menjadi lebih ragu dalam menggunakan layanan transaksi elektronik karena khawatir data pribadinya kembali disalahgunakan. Kondisi ini menunjukkan bahwa phishing bukan sekadar bentuk penipuan biasa, melainkan ancaman serius terhadap stabilitas ekosistem digital di Indonesia.

Kasus-kasus phishing yang terus meningkat menegaskan perlunya langkah pencegahan yang lebih komprehensif. Upaya tersebut tidak hanya melalui penguatan regulasi dan penindakan hukum, tetapi juga melalui peningkatan literasi digital masyarakat agar pengguna mampu mengenali ciri-ciri tautan palsu, memahami pentingnya menjaga kerahasiaan data pribadi, serta memiliki kesadaran untuk selalu melakukan verifikasi sebelum mengakses suatu tautan digital. Dengan demikian, ruang digital dapat menjadi lebih aman dari ancaman kejahatan siber yang terus berkembang.

Upaya Pencegahan dan Penanggulangan Praktik Phishing di Era Digital

Upaya pencegahan dan penanggulangan phishing tidak dapat dilakukan hanya melalui penegakan hukum, tetapi harus disertai penguatan kesadaran digital masyarakat. Tingginya intensitas penggunaan layanan berbasis internet menuntut setiap pengguna memiliki kemampuan untuk mengenali ciri-ciri tautan palsu, memahami risiko penyalahgunaan data pribadi, serta membiasakan diri melakukan verifikasi sebelum mengakses suatu tautan digital. Literasi keamanan digital menjadi langkah paling mendasar dalam menekan keberhasilan praktik phishing, sebab sebagian besar serangan memanfaatkan kelengahan dan kurangnya pengetahuan pengguna dalam menjaga keamanan informasi pribadi. Selain peningkatan literasi digital, penguatan sistem keamanan teknologi juga menjadi langkah penting. Penyedia layanan digital perlu menerapkan sistem perlindungan berlapis, seperti autentikasi dua faktor, enkripsi data, serta deteksi otomatis terhadap aktivitas mencurigakan. Langkah ini bertujuan mempersempit ruang gerak pelaku sekaligus meminimalkan potensi kebocoran data apabila terjadi upaya serangan digital.

Dari sisi hukum, diperlukan penegakan aturan yang adaptif terhadap perkembangan kejahatan siber. Aparat penegak hukum harus didukung kemampuan teknis yang memadai agar dapat mendeteksi, melacak, dan menindak pelaku phishing secara efektif, termasuk ketika kejahatan dilakukan lintas wilayah melalui identitas anonim. Penegakan hukum yang tegas akan memberikan efek pencegahan sekaligus memperkuat kepercayaan masyarakat terhadap keamanan ruang digital. Pencegahan phishing membutuhkan sinergi antara masyarakat, penyedia layanan digital, dan aparat penegak hukum. Kolaborasi tersebut menjadi kunci utama dalam menciptakan ekosistem digital yang aman serta menekan perkembangan phishing sebagai salah satu bentuk kriminalitas kontemporer di era digital.

SIMPULAN

Phishing melalui tautan digital palsu merupakan salah satu bentuk kriminalitas kontemporer yang berkembang seiring pesatnya digitalisasi masyarakat. Kejahatan ini memanfaatkan kemajuan teknologi, rendahnya literasi digital, serta lemahnya kesadaran masyarakat terhadap keamanan data pribadi untuk memperoleh keuntungan secara ilegal. Dalam perspektif kriminologi, phishing menunjukkan adanya pergeseran pola kejahatan dari konvensional menuju kejahatan modern berbasis ruang siber yang lebih anonim dan sulit

dideteksi. Oleh karena itu, penanggulangannya memerlukan penguatan literasi digital, peningkatan sistem keamanan teknologi, serta penegakan hukum yang adaptif agar tercipta ruang digital yang aman dan terpercaya bagi masyarakat.

DAFTAR RUJUKAN

Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4(1), 165-189.

Benuf, K., & Azhar, M. (2020). Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. Gema Keadilan, 7(1).

Fatiha, M. R. (2024). Optimisasi Sistem Deteksi Phishing Berbasis Artificial Intelligence.

Fauzi, A. (2024). Ketergantungan Digital dan Ancaman Kejahatan Siber di Indonesia.

Latifahi, F. N., Mawardi, I., & Wardhana, B. (2022). Ancaman Pencurian Data (Phishing) di Tengah Trend Pengguna Fintech pada Pandemic Covid-19.

Nurhayati, Y., Ifrani, I., & Said, M. Y. (2021). Metodologi Normatif dan Empiris dalam Perspektif Ilmu Hukum. Jurnal Penegakan Hukum Indonesia, 2(1).

Purwandari, M. D. (2024). Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus Phishing (Doctoral dissertation, Universitas Islam Indonesia).

Ramadhan, M. K. (2022). Transformasi Cybercrime dalam Era Digital di Indonesia.

Sahfitri, A., & Rosmalinda, R. (2024). Penipuan Digital Melalui Tautan Phishing. Jurnal Dialektika Hukum, 6(2), 92-107.

Salsabila, N. (2025). Apa itu phishing? Pengertian, jenis, dan cara menghindarinya. Mekari Sign. Diakses pada 15 Mei 2026, dari https://mekarisign.com/id/blog/apa-itu-phising/

Tan, D. (2021). Metode Penelitian Hukum: Mengupas dan Mengulas Metodologi dalam Menyelenggarakan Penelitian Hukum. Nusantara: Jurnal Ilmu Pengetahuan Sosial, 8(8).

Wijaya, R. (2023). Cyber Law dan Tantangan Penegakan Hukum di Era Digital.

Wiraguna, S. (2024). Metode Normatif dan Empiris dalam Penelitian Hukum: Studi Eksploratif di Indonesia. Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum, 3(3).

