Volume 6, Isu 1, Tahun 2026, ISSN: 2808-7089 (Online), doi: 10.21274
Jurnal Penelitian Mahasiswa Ilmu Sosial, Ekonomi, dan Bisnis Islam (SOSEBI)
Fakultas Ekonomi dan Bisnis Islam
Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung
Jl. Mayor Sujadi Timur No. 46 Tulungagung Jawa Timur 66221 Indonesia
Website: https://ejournal.uinsatu.ac.id/index.php/sosebi/index

FENOMENA PENIPUAN *LINK PHISHING* DALAM PERSPEKTIF SOSIOLOGI KRIMINALITAS

Nur Humaira[1*], Phoja Aulia Cahyani Munthe[2], Ahmadi Ridho Baihaqi[3], Hendrik[4], Endri Bagus Prastiyo[5]
[1,2,3,4]Mahasiswa Jurusan Sosiologi, STISIPOL Raja Haji Tanjungpinang
[5]Dosen Jurusan Sosiologi, STISIPOL Raja Haji Tanjungpinang
[*]Email: nurhumaira.ard@gmail.com

Abstrak: *Perkembangan teknologi digital yang pesat telah membuka peluang terjadinya berbagai bentuk kejahatan siber, salah satunya penipuan berbasis phishing. Fenomena ini terus mengalami peningkatan yang signifikan, berdasarkan data Indonesia Domain Abuse Data Exchange (IDADX) mencatat 2.470 laporan phishing pada kuartal pertama tahun 2025 dan meningkat menjadi 3.138 kasus pada kuartal pertama tahun 2026. Penelitian ini bertujuan untuk mendeskripsikan fenomena penipuan phishing di Indonesia, menganalisis motif pelaku melalui perspektif sosiologi kriminalitas, serta mengidentifikasi faktor-faktor sosiologis yang memengaruhi kerentanan korban terhadap penipuan phishing. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kepustakaan. Sumber data terdiri dari artikel jurnal ilmiah, laporan lembaga resmi seperti IDADX, BSSN, dan OJK, serta berita dari media terpercaya yang relevan dengan topik penelitian. Analisis data dilakukan menggunakan metode analisis isi dengan mengacu pada kerangka Teori Anomie, Teori Kontrol Sosial, Teori Differential Association, dan Teori Aktivitas Rutin. Hasil penelitian menunjukkan bahwa motif pelaku phishing dapat dijelaskan melalui tiga teori, yakni tekanan struktural antara tujuan finansial dan keterbatasan akses sarana yang sah (Teori Anomie), lemahnya ikatan sosial yang mendorong pelaku beroperasi secara anonim (Teori Kontrol Sosial), serta proses pembelajaran kejahatan melalui komunitas digital (Teori Differential Association). Sementara itu, kerentanan korban dijelaskan melalui Teori Aktivitas Rutin, yakni tingginya intensitas aktivitas digital masyarakat yang tidak diimbangi dengan literasi dan kewaspadaan digital yang memadai. Penelitian ini menegaskan bahwa penanggulangan phishing memerlukan pendekatan multi-dimensi yang melampaui aspek hukum dan teknis semata.*

Kata Kunci: *phishing; sosiologi kriminalitas; teori anomie; teori kontrol sosial; teori aktivitas rutin.*

Abstract: *The rapid development of digital technology has opened opportunities for various forms of cybercrime, one of which is phishing-based fraud. This phenomenon has continued to increase significantly, with data from the Indonesia Domain Abuse Data Exchange (IDADX) recording 2,470 phishing reports in the first quarter of 2025, rising to 3,138 cases in the first quarter of 2026. This study aims to describe the phenomenon of phishing fraud in Indonesia, analyze the perpetrators' motives through the perspective of criminal sociology, and identify sociological factors that influence victims' vulnerability to phishing fraud. This study employs a qualitative approach using a library research method. Data sources consist of scientific journal articles, official institutional reports from IDADX, BSSN, and OJK, as well as relevant news from credible media. Data analysis was conducted using content analysis referring to the frameworks of Anomie Theory, Social Control Theory, Differential Association Theory, and Routine Activity Theory. The results show that the motives of phishing perpetrators can be explained through three theories: structural pressure between financial goals and limited access to legitimate means (Anomie Theory), weak social bonds that drive perpetrators to operate anonymously (Social Control Theory), and the process of learning criminal behavior through digital communities (Differential Association Theory). Meanwhile, victims' vulnerability is explained through Routine Activity Theory, namely the high intensity of digital activity in society that is not matched by adequate digital literacy and vigilance. This study concludes that combating phishing requires a multi-dimensional approach that goes beyond legal and technical aspects alone.*
Keywords: *phishing; criminal sociology; anomie theory; social control theory; routine activity theory.*

PENDAHULUAN

Perkembangan teknologi digital telah membawa berbagai kemudahan dalam kehidupan masyarakat, terutama dalam bidang komunikasi dan transaksi ekonomi. Namun, di sisi lain, kemajuan ini juga membuka peluang terjadinya berbagai bentuk kejahatan siber, salah satunya adalah penipuan berbasis *phishing*. *Phishing* merupakan salah satu bentuk kejahatan yang dilakukan dengan cara memanipulasi korban melalui tautan atau situs palsu guna memperoleh data pribadi, seperti informasi akun, kata sandi, hingga data keuangan (Trianurahmah, Fauzi, Tyas, & Suryanto, 2025).

Fenomena penipuan *phishing* di Indonesia menunjukkan peningkatan yang sangat signifikan dari tahun ke tahun. Berdasarkan laporan Indonesia Domain Abuse Data Exchange (IDADX), ancaman *phishing* terus mengalami eskalasi yang mengkhawatirkan, pada kuartal pertama tahun 2025 tercatat sebanyak 2.470 laporan *phishing* (IDADX, 2025). Jumlah ini meningkat kembali menjadi 3.138 kasus pada kuartal pertama tahun 2026 (IDADX, 2026). Lonjakan yang konsisten dari tahun ke tahun ini menegaskan bahwa kejahatan *phishing* telah menjadi ancaman serius dan berkelanjutan bagi keamanan sistem digital nasional, dengan

sektor keuangan dan platform digital sebagai target yang paling dominan. Modus operandi pelaku melibatkan berbagai media yang terhubung ke internet, seperti email, SMS, dan situs web, dengan cara menawarkan hadiah palsu guna memancing target mengklik tautan yang mengarah pada peretasan data pribadi (Iskandar, 2024).

Kondisi ini diperparah oleh kurangnya literasi digital serta kelengahan korban yang dimanfaatkan oleh pelaku untuk melancarkan aksinya. Sebagian besar penelitian terdahulu cenderung menempatkan *phishing* hanya dalam perspektif hukum dan teknis keamanan informasi. Padahal, praktik ini juga merupakan fenomena sosial yang melibatkan interaksi kompleks antara pelaku, korban, dan lingkungan digital. Dengan demikian, pendekatan sosiologi kriminalitas menjadi krusial untuk memahami *phishing* secara lebih komprehensif, khususnya dalam mengkaji motif di balik tindakan pelaku.

Dalam kajian sosiologi kriminalitas, tindakan *phishing* tidak hanya dipandang sebagai pelanggaran hukum semata, tetapi juga sebagai hasil dari berbagai faktor sosial yang memengaruhi perilaku individu. Berbagai teori seperti teori aktivitas rutin, teori kontrol sosial dan *Strain Theory* dapat digunakan sebagai pisau analisis untuk membedah motif di balik tindakan kriminal ini. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mendeskripsikan konsep *phishing* dalam konteks digital, menganalisis motif pelaku melalui perspektif sosiologi kriminalitas, serta mengidentifikasi faktor-faktor sosiologis yang memengaruhi kerentanan korban terhadap penipuan *phishing*.

KAJIAN PUSTAKA

Pengertian *Phishing*

Phishing berasal dari kata *fishing* yang berarti “memancing”. Istilah ini digunakan untuk menggambarkan tindakan pelaku kejahatan siber yang “memancing” korban agar secara sukarela memberikan informasi pribadi dan data sensitif mereka. Dalam praktiknya, *phishing* dilakukan dengan cara menipu atau mengelabui korban melalui pesan persuasif yang tampak berasal dari pihak resmi, seperti bank, lembaga pemerintah, institusi pendidikan, maupun penyedia layanan digital. Korban biasanya diarahkan untuk mengklik tautan, membuka lampiran, atau mengisi data pada situs palsu yang menyerupai situs asli (Sahfitri & Rosmalinda, 2024). *Phishing* juga merupakan salah satu bentuk kejahatan siber yang menggunakan teknik rekayasa sosial (*social engineering*) untuk memperoleh data pribadi korban. Pelaku *phishing* atau phisher berusaha mendapatkan informasi penting seperti *username*, kata sandi, data rekening, hingga informasi kartu kredit yang nantinya dapat digunakan untuk pencurian identitas maupun pengambilalihan akun korban (Vadila & Pratama, 2021).

Selain melalui *website* palsu, *phishing* juga banyak dilakukan melalui email maupun media sosial seperti WhatsApp, Telegram, dan Facebook. Pesan yang dikirim biasanya mengandung unsur urgensi atau ancaman sehingga korban terdorong untuk segera mengikuti instruksi yang diberikan tanpa melakukan verifikasi terlebih dahulu. Ketika korban mengklik tautan atau mengunduh dokumen tertentu, pelaku dapat memperoleh akses terhadap perangkat maupun akun pribadi korban secara otomatis (Sahfitri & Rosmalinda, 2024). Informasi yang berhasil diperoleh, seperti identitas pribadi, data perbankan, PIN ATM, maupun data kartu kredit, kemudian digunakan untuk kepentingan kriminal seperti pencurian dana, penyalahgunaan identitas, hingga penjualan data di pasar gelap digital (*dark web*). Modus yang digunakan umumnya berupa pembuatan *website* palsu yang dirancang semirip mungkin dengan tampilan asli agar mampu menarik perhatian dan meyakinkan calon korban untuk memasukkan data pribadinya (Sahfitri & Rosmalinda, 2024).

Sosiologi Kriminalitas

Sosiologi kriminalitas merupakan cabang ilmu sosiologi yang secara khusus mempelajari kejahatan sebagai fenomena sosial dengan mengkaji sebab-sebab, pola, dan dampak kejahatan dalam konteks kehidupan bermasyarakat (Maulida, 2025). Berbeda dengan pendekatan hukum yang memandang kejahatan dari sudut normatif, sosiologi kriminalitas berupaya memahami mengapa kejahatan terjadi dengan menelaah faktor-faktor sosial yang melatarbelakanginya, seperti struktur sosial, ketimpangan ekonomi, lingkungan pergaulan, hingga lemahnya kontrol sosial dalam masyarakat

Bidang kajian ini tidak hanya berfokus pada pelaku kejahatan, tetapi juga memperhatikan relasi antara pelaku, korban, dan kondisi sosial yang memungkinkan suatu kejahatan terjadi (Azis & Ridwan, 2025). Seiring perkembangan zaman, sosiologi kriminalitas terus beradaptasi dalam menganalisis bentuk-bentuk kejahatan baru, termasuk kejahatan yang berkembang di ruang digital (*cybercrime*), dengan tetap menggunakan kerangka teori sosial sebagai landasan analisisnya (Butarbutar, 2025).

Teori Aktivitas Rutin

Teori Aktivitas Rutin yang diperkenalkan oleh Cohen dan Felson (1979) menjelaskan bahwa kejahatan terjadi ketika tiga elemen bertemu secara bersamaan, yakni pelaku yang termotivasi (*motivated offender*), target yang sesuai (*suitable target*), dan ketiadaan penjaga yang cakap (*absence of capable guardian*). Teori ini menekankan bahwa kejahatan tidak selalu disebabkan oleh karakter buruk pelaku, tetapi juga sangat dipengaruhi oleh adanya kesempatan

yang memungkinkan tindak kriminal terjadi. Perubahan pola aktivitas rutin masyarakat, seperti meningkatnya penggunaan internet untuk transaksi keuangan dan komunikasi, secara tidak langsung dapat memperluas peluang bagi pelaku kejahatan untuk menemukan target yang sesuai (Ichsan, 2021).

Teori Strain/Anomie

Teori Anomie yang dikembangkan oleh Robert K. Merton pada tahun 1938 menjelaskan bahwa kejahatan muncul akibat adanya ketegangan (*strain*) antara tujuan-tujuan sosial yang diinginkan masyarakat dengan sarana-sarana yang tersedia untuk mencapainya. Merton berpendapat bahwa masyarakat menanamkan tujuan-tujuan tertentu, seperti kesuksesan finansial dan status sosial, namun tidak semua individu memiliki akses yang sama terhadap cara-cara yang sah (*legitimate means*) untuk meraih tujuan tersebut. Kondisi ketidakseimbangan inilah yang disebut Merton sebagai anomie, yaitu keadaan ketika norma-norma sosial kehilangan kekuatannya dalam mengendalikan perilaku individu. Ketika individu mengalami tekanan struktural ini, mereka cenderung merespons dengan berbagai cara, salah satunya adalah *innovation*, yakni tetap mengejar tujuan yang diinginkan masyarakat namun menggunakan cara-cara yang menyimpang atau ilegal.

Dalam konteks kejahatan siber, respons inilah yang relevan untuk menjelaskan perilaku pelaku *phishing* yang memilih jalan pintas melalui penipuan digital sebagai cara untuk memperoleh keuntungan finansial yang tidak dapat mereka raih melalui jalur yang sah. Dengan demikian, Teori Anomie memberikan pemahaman bahwa akar dari kejahatan *phishing* tidak semata-mata berasal dari niat jahat individu, melainkan juga dari ketimpangan struktural dalam masyarakat yang mendorong sebagian individu untuk mencari alternatif di luar batas norma yang berlaku (Azis & Ridwan, 2025)

Teori Kontrol Sosial

Teori Kontrol Sosial yang dikemukakan oleh Travis Hirschi pada tahun 1969 dalam karyanya *Causes of Delinquency* berpandangan bahwa setiap individu pada dasarnya memiliki potensi untuk melakukan kejahatan, dan yang menjadi pertanyaan bukan mengapa seseorang melakukan kejahatan, melainkan mengapa kebanyakan orang tidak melakukannya. Hirschi berargumen bahwa perilaku menyimpang dapat dicegah melalui ikatan sosial (*social bond*) yang kuat antara individu dengan masyarakatnya. Ikatan sosial tersebut terdiri dari empat elemen, yaitu *attachment* (keterikatan emosional dengan orang-orang di sekitar), *commitment* (komitmen terhadap tujuan-tujuan konvensional seperti pendidikan dan karier), *involvement*

(keterlibatan dalam aktivitas sosial yang positif), dan *belief* (kepercayaan terhadap nilai dan norma yang berlaku dalam masyarakat). Ketika salah satu atau beberapa elemen ikatan sosial tersebut melemah atau putus, individu menjadi lebih rentan untuk terlibat dalam perilaku kriminal karena tidak ada lagi kontrol yang cukup kuat untuk menahan dorongan tersebut (Dewi, 2025).

Dalam konteks penipuan *phishing*, lemahnya ikatan sosial dapat menjelaskan mengapa sebagian individu memilih untuk memanfaatkan anonimitas dunia digital sebagai ruang untuk melakukan penipuan tanpa merasa terikat oleh norma sosial yang berlaku di kehidupan nyata. Dengan demikian, Teori Kontrol Sosial menegaskan bahwa pencegahan kejahatan siber seperti *phishing* tidak hanya bergantung pada sistem hukum formal, tetapi juga pada kuatnya ikatan sosial dan internalisasi nilai-nilai moral dalam diri setiap individu.

Teori Differential Association

Teori *Differential Association* dikemukakan oleh Edwin H. Sutherland pada tahun 1939 dan dikembangkan lebih lanjut dalam karyanya *Principles of Criminology*. Teori ini berpandangan bahwa perilaku kriminal bukanlah sesuatu yang bersifat bawaan, melainkan dipelajari melalui proses interaksi sosial dengan orang-orang di sekitar individu tersebut. Sutherland berargumen bahwa seseorang menjadi pelaku kejahatan bukan karena faktor biologis atau psikologis semata, melainkan karena ia lebih banyak terpapar pada definisi-definisi yang mendukung pelanggaran hukum dibandingkan definisi yang menentangnya. Semakin intens, sering, dan lama seseorang berinteraksi dengan lingkungan atau kelompok yang menganggap kejahatan sebagai sesuatu yang wajar atau menguntungkan, maka semakin besar pula kemungkinan individu tersebut terlibat dalam perilaku kriminal (Azis & Ridwan, 2025).

Dalam konteks kejahatan siber, Teori *Differential Association* sangat relevan untuk menjelaskan bagaimana pelaku *phishing* mempelajari teknik-teknik penipuan digital melalui interaksi dengan komunitas atau jaringan kejahatan siber, baik secara langsung maupun melalui forum-forum daring seperti *dark web* dan platform terenkripsi. Paparan terhadap komunitas yang menormalisasi kejahatan siber sebagai cara memperoleh penghasilan, berbagi *script phishing*, dan saling mengajarkan modus operandi baru, secara perlahan membentuk orientasi nilai pelaku yang memandang *phishing* bukan sebagai kejahatan, melainkan sebagai keahlian atau bisnis. Dengan demikian, Teori *Differential Association* menegaskan bahwa penyebaran

kejahatan *phishing* juga dipahami sebagai fenomena pembelajaran sosial yang terjadi dalam ekosistem komunitas digital yang tertutup dan terorganisir.

Penelitian Terdahulu

Sejumlah penelitian sebelumnya telah mengkaji fenomena *phishing* dari perspektif hukum dan regulasi. Penelitian yang berjudul "Penipuan Digital melalui Tautan *Phishing*" menyimpulkan bahwa penipuan digital melalui tautan *phishing* merupakan tindak pidana yang diatur dalam Pasal 378 KUHP dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, dengan upaya penanggulangan yang ditekankan pada peningkatan literasi digital masyarakat serta penguatan kerja sama dalam penegakan hukum (Sahfitri & Rosmalinda, 2024). Sementara itu, penelitian yang berjudul "Analisis Penipuan Online melalui Media Sosial dalam Perspektif Kriminologi" mengkaji fenomena penipuan online termasuk *phishing* dari sudut pandang yuridis normatif, dengan menyimpulkan bahwa tindak pidana penipuan online diatur dalam Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE dengan ancaman pidana penjara hingga enam tahun dan/atau denda hingga satu miliar rupiah (Mulyadi, Nurdin, Anjani, & Fiqih, 2024).

Kedua penelitian tersebut memberikan kontribusi penting dalam memahami fenomena *phishing* dari aspek hukum dan regulasi. Namun, keduanya belum mengkaji fenomena *phishing* secara mendalam dari perspektif sosiologi kriminalitas. Berbeda dengan penelitian sebelumnya yang lebih berfokus pada aspek yuridis normatif, penelitian ini secara khusus menganalisis fenomena penipuan *phishing* menggunakan kerangka teori sosiologi kriminalitas, yakni Teori Anomie, Teori Kontrol Sosial, dan Teori Aktivitas Rutin. Dengan demikian, penelitian ini diharapkan dapat melengkapi kajian yang telah ada dengan memberikan pemahaman yang lebih komprehensif mengenai akar sosial dari kejahatan *phishing* di luar aspek hukum semata.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kepustakaan (*library research*). Pendekatan kualitatif dipilih karena penelitian ini bertujuan untuk memahami dan menganalisis fenomena penipuan *phishing* secara mendalam melalui kerangka teori sosiologi kriminalitas, bukan untuk mengukur variabel secara statistik. Metode studi kepustakaan dilakukan dengan mengkaji, menganalisis, dan mensintesis berbagai sumber tertulis yang relevan dengan topik penelitian, seperti artikel jurnal ilmiah, buku, laporan lembaga resmi, serta dokumen digital yang dapat dipertanggungjawabkan kredibilitasnya.

Sumber data dalam penelitian ini terdiri dari dua jenis, yaitu sumber data primer dan sumber data sekunder. Sumber data primer meliputi artikel jurnal ilmiah yang secara langsung membahas fenomena *phishing* maupun teori-teori sosiologi kriminalitas yang digunakan sebagai kerangka analisis. Sementara itu, sumber data sekunder meliputi laporan dari lembaga terkait seperti Indonesia *Anti-Phishing* Data *Exchange* (IDADX), Badan Siber dan Sandi Negara (BSSN), serta berbagai referensi pendukung lainnya yang relevan dengan topik penelitian.

Teknik pengumpulan data dilakukan melalui identifikasi, seleksi, dan dokumentasi sumber-sumber pustaka yang relevan. Sumber-sumber tersebut ditelusuri melalui berbagai basis data ilmiah seperti Google Scholar, serta situs resmi lembaga yang berkaitan dengan keamanan siber di Indonesia. Adapun prosedur analisis data yang digunakan adalah analisis isi (*content analysis*), yakni dengan membaca secara kritis, mengklasifikasikan, dan menginterpretasikan data yang diperoleh dari berbagai sumber pustaka untuk kemudian dikaitkan dengan kerangka teori yang digunakan, yaitu Teori *Anomie*, Teori Kontrol Sosial, dan Teori Aktivitas Rutin.

HASIL DAN PEMBAHASAN

Gambaran Umum Fenomena *Phishing* di Indonesia

Fenomena penipuan *phishing* di Indonesia telah berkembang menjadi ancaman siber yang semakin serius dan tidak dapat diabaikan. Pesatnya pertumbuhan pengguna internet di Indonesia, yang kini mencapai ratusan juta pengguna aktif, telah menciptakan ekosistem digital yang subur sekaligus rentan terhadap berbagai bentuk kejahatan siber. Berdasarkan laporan IDADX, jumlah laporan *phishing* mengalami peningkatan yang sangat signifikan, pada kuartal pertama tahun 2023 tercatat sebanyak 26.675 laporan, melonjak drastis dari hanya 6.106 laporan pada kuartal keempat tahun 2022, atau meningkat sebanyak 20.569 laporan hanya dalam satu kuartal saja (IDADX, 2023). Lonjakan angka yang begitu tajam dalam waktu singkat ini mencerminkan betapa cepatnya pelaku kejahatan siber beradaptasi dan memanfaatkan celah keamanan digital yang ada di masyarakat.

Tren peningkatan ini tidak hanya tercermin dalam data IDADX, tetapi juga dikonfirmasi oleh berbagai lembaga otoritatif lainnya. BSSN melaporkan adanya peningkatan sebesar 70 persen pada kasus *phishing* selama tahun 2024 dibandingkan tahun 2023, dengan dampak yang dirasakan secara finansial maupun emosional oleh banyak masyarakat Indonesia (Farhansyah, 2025). Angka ini menunjukkan bahwa kejahatan *phishing* bukan sekadar

ancaman yang bersifat teknis, melainkan telah menjadi persoalan sosial yang berdampak nyata pada kesejahteraan dan keamanan masyarakat secara luas. Di tingkat global, perusahaan keamanan siber Kaspersky mencatat peningkatan serangan *phishing* sebesar 40 persen sepanjang tahun 2023, dengan total mencapai lebih dari 709 juta upaya serangan *phishing* di seluruh dunia (CNN Indonesia, 2024). Fakta bahwa tren global ini turut dirasakan secara intens di Indonesia menunjukkan bahwa Indonesia merupakan salah satu negara yang paling terdampak oleh gelombang kejahatan siber jenis ini. Hal tersebut sejalan dengan posisi Indonesia di kancah global, saat ini Indonesia menduduki posisi kedua sebagai sasaran utama serangan siber canggih di kawasan Asia Pasifik, dengan serangan yang tidak hanya bersifat individual melainkan juga terkait operasi spionase, ransomware, dan pemanfaatan kecerdasan buatan oleh penjahat siber.

Tren ancaman *phishing* terus menunjukkan eskalasi yang mengkhawatirkan hingga tahun-tahun terkini. Berdasarkan data IDADX pada kuartal I tahun 2025, kategori phishing tetap mendominasi laporan dengan total 2.470 kasus, dengan sepuluh entitas yang paling banyak dijadikan target impersonasi antara lain Dana, Telegram, Bank Mandiri, Facebook, Zoetis, Instagram, Tencent, Shopee, WhatsApp, hingga situs-situs perjudian daring (IDADX, 2025). Pemilihan target-target tersebut bukanlah tanpa alasan, melainkan mencerminkan strategi pelaku yang secara kalkulatif menyasar platform-platform dengan jumlah pengguna terbesar di Indonesia, sehingga peluang keberhasilan penipuan menjadi jauh lebih tinggi. Data terbaru dari kuartal I tahun 2026 menunjukkan eskalasi yang lebih mengkhawatirkan lagi, pada kategori *phishing* mencapai 3.138 kasus, diikuti oleh perjudian daring sebanyak 1.165 kasus (IDADX, 2026). Distribusi ini mengindikasikan bahwa lebih dari 85-90% penyalahgunaan domain didorong oleh motif ekonomi melalui penipuan dan aktivitas ilegal lainnya, sebuah gambaran yang menegaskan betapa kuatnya dimensi finansial sebagai pendorong utama kejahatan siber di Indonesia.

Dari segi sektor yang menjadi sasaran, pola ancaman *phishing* menunjukkan konsistensi yang jelas dan sistematis. Pada kuartal pertama tahun 2023, sektor media sosial menjadi sasaran terbanyak dengan persentase 45%, diikuti oleh sektor lembaga keuangan sebesar 31%, ritel atau *e-commerce* sebanyak 20%, serta sektor lainnya seperti ISP dan mata uang kripto (IDADX, 2023). Memasuki kuartal I tahun 2025, terjadi pergeseran pola yang signifikan sehingga sektor keuangan mengambil alih posisi teratas dengan persentase 50,98%, disusul sektor jejaring sosial sebesar 25,74%. Pergeseran ini mencerminkan semakin matangnya strategi pelaku yang kini lebih berfokus pada sektor dengan potensi keuntungan finansial langsung yang lebih besar (IDADX, 2025). Data kuartal I tahun 2026 memperkuat

pola ini, dengan sektor finansial tetap menjadi target utama yang berkontribusi sebesar 36,3%, diikuti sektor merce/retail sebesar 24,4%, gaming sebesar 13,5%, ISP/teknologi sebesar 12,9%, dan jejaring sosial sebesar 9,5% (IDADX, 2026).

Modus operandi yang digunakan pelaku *phishing* di Indonesia pun terus berkembang menjadi semakin beragam dan canggih seiring waktu. Latar belakang serangan *phishing* di Indonesia beragam, sebagian bermotif ekonomi seperti mengincar rekening korban, sebagian lagi bermotif politis dengan tujuan mengambil alih akun korban, dengan jenisnya mulai dari tautan di aplikasi percakapan atau surel hingga *phishing* menggunakan Android Package Kit (APK). Pelaku tidak lagi hanya mengandalkan email palsu konvensional, tetapi telah merambah berbagai platform digital yang akrab digunakan masyarakat sehari-hari, mulai dari pesan singkat di WhatsApp dan Telegram, kolom komentar media sosial, hingga aplikasi palsu yang dirancang menyerupai aplikasi resmi (Trianurahmah, Fauzi, Tyas, & Suryanto, 2025). Kecanggihan modus ini diperparah oleh fakta bahwa pelaku semakin mahir dalam memanfaatkan rekayasa sosial (social engineering) untuk mengeksploitasi kepercayaan dan kelengahan korban, sehingga pengguna yang relatif memiliki tingkat literasi digital yang baik pun tidak sepenuhnya terbebas dari risiko menjadi korban *phishing*. Kondisi ini menegaskan bahwa fenomena *phishing* di Indonesia bukan semata-mata persoalan teknis keamanan siber, melainkan juga merupakan fenomena sosial yang memerlukan pendekatan analisis yang lebih komprehensif, termasuk melalui perspektif sosiologi kriminalitas.

Analisis Motif Pelaku *Phishing* Berdasarkan Teori Sosiologi Kriminalitas

Analisis terhadap motif pelaku *phishing* di Indonesia dapat dipahami secara komprehensif melalui tiga kerangka teori sosiologi kriminalitas, yakni Teori Anomie, Teori Kontrol Sosial, dan Teori *Differential Association*. Ketiga teori ini saling melengkapi dalam menjelaskan mengapa seseorang memilih untuk terlibat dalam kejahatan *phishing*, bukan hanya dari sisi karakter individu, melainkan juga dari tekanan struktural dan pengaruh lingkungan sosialnya.

Dari perspektif Teori Anomie Merton, motif pelaku *phishing* sangat erat kaitannya dengan ketimpangan antara tujuan finansial yang diinginkan dan terbatasnya akses terhadap cara-cara yang sah untuk mencapainya. Hal ini tampak jelas dalam kasus *phishing* undangan pernikahan digital yang terungkap pada Januari 2023. Pelaku berinisial AI (20 tahun), seorang mahasiswa warga Kabupaten Pinrang, Sulawesi Selatan, memproduksi dan menjual file APK berkedok "Surat Undangan Pernikahan Digital," sehingga para pembeli kemudian

menggunakan APK tersebut untuk melakukan kejahatan serupa terhadap lebih dari satu korban, hingga pelaku divonis 1 tahun penjara setelah terbukti merugikan korban setidaknya Rp95,9 juta (CNN Indonesia, 2024). Dalam perspektif Teori Anomie, AI merepresentasikan individu muda yang memiliki tujuan finansial sebagaimana ditanamkan masyarakat, namun tidak memiliki akses memadai terhadap sarana-sarana yang sah seperti pekerjaan tetap atau jalur karier formal. Kondisi ketimpangan inilah yang mendorong ia memilih respons *innovation* dalam tipologi Merton, yakni tetap mengejar tujuan finansial namun melalui cara-cara yang menyimpang. Kasus serupa juga terlihat pada pengungkapan sindikat *phishing tools* lintas negara oleh Bareskrim Polri pada April 2026 (Tim detikcom, 2026). Tersangka utama berinisial GWL berusia 24 tahun, hanya berlatar belakang lulusan SMK Multimedia yang mengembangkan keahlian membuat *script* secara autodidak, namun berhasil membangun jaringan kejahatan siber internasional yang diperkirakan meraup keuntungan hingga Rp25 miliar sepanjang periode 2019 hingga 2024. Profil GWL yang hanya berpendidikan SMK, tanpa akses terhadap pendidikan tinggi maupun karier formal, tetapi memiliki kemampuan teknis yang tinggi, mencerminkan kondisi anomie sebagaimana dikemukakan oleh Merton. Kondisi ini muncul ketika individu menghadapi kesenjangan antara tujuan yang diharapkan secara sosial dan keterbatasan sarana yang tersedia untuk mencapainya, sehingga mendorong pencarian alternatif di luar jalur yang dianggap normatif.

Teori Kontrol Sosial Hirschi memberikan lensa analisis yang berbeda dengan menekankan bahwa lemahnya ikatan sosial individu menjadi faktor penentu keterlibatan seseorang dalam perilaku kriminal. Kembali mengacu pada kasus GWL dan kekasihnya FYT (25 tahun), dimensi kontrol sosial tampak dari cara keduanya menjalankan operasi kejahatan secara anonim dan tersembunyi (Tim detikcom, 2026). Dalam menjalankan bisnis ilegalnya, kedua tersangka menggunakan layanan *virtual private server* (VPS) yang berada di luar negeri dan memanfaatkan bot Telegram sebagai sarana komunikasi serta pengiriman *script* kepada para pembeli, beroperasi sepenuhnya di balik anonimitas dunia digital. Pilihan untuk bersembunyi di balik anonimitas ini mencerminkan lemahnya elemen *belief* dalam ikatan sosial keduanya, yakni tidak adanya kepercayaan terhadap nilai dan norma yang berlaku, sehingga mereka tidak merasa terikat oleh konsekuensi sosial atas tindakannya. Usia keduanya yang masih sangat muda tanpa jejak karier formal maupun keterlibatan aktif dalam institusi sosial konvensional juga mengindikasikan lemahnya elemen *commitment* dan *involvement* sebagaimana dirumuskan Hirschi. Kondisi ini menegaskan bahwa dunia digital telah menciptakan ruang baru bagi pelaku kejahatan dapat bertindak tanpa merasa diawasi oleh

lingkungan sosialnya, sehingga dorongan untuk menyimpang tidak lagi terbendung oleh ikatan sosial yang seharusnya berfungsi sebagai rem moral.

Dimensi lain yang tak kalah penting dalam memahami motif pelaku *phishing* adalah perspektif Teori *Differential Association* Sutherland, yang menekankan bahwa perilaku kriminal dipelajari melalui proses interaksi sosial. Kasus *phishing* APK undangan pernikahan memberikan ilustrasi yang sangat gamblang mengenai proses pembelajaran kejahatan ini (CNN Indonesia, 2024). Setelah AI memproduksi APK berbahaya tersebut, ia kemudian menjualnya kepada pembeli lain yang selanjutnya menggunakan APK tersebut untuk melancarkan aksi kejahatan serupa terhadap korban-korban baru, bahkan penangkapan turut dilakukan di Sumatera dan di Wajo. Fenomena ini memperlihatkan bagaimana kejahatan *phishing* tidak berhenti pada satu pelaku, melainkan menyebar melalui jaringan sosial digital layaknya sebuah proses pembelajaran kolektif. Para pembeli APK mempelajari teknik *phishing* bukan melalui pendidikan formal, melainkan melalui interaksi dengan komunitas yang menormalisasi dan bahkan mengkomersialisasikan kejahatan siber sebagai sumber penghasilan. Di Indonesia, fenomena serupa juga terlihat pada munculnya komunitas-komunitas daring yang saling berbagi teknik penipuan digital, sehingga pelaku *phishing* semakin canggih dalam memanfaatkan layanan populer seperti Telegram untuk menjebak korban. Dengan demikian, Teori *Differential Association* menegaskan bahwa semakin seseorang terpapar pada lingkungan yang mendefinisikan kejahatan *phishing* sebagai sesuatu yang wajar dan menguntungkan, semakin besar pula kemungkinan individu tersebut terlibat dan bahkan turut menyebarkan kejahatan tersebut kepada orang lain di sekitarnya.

Faktor Kerentanan Korban terhadap Penipuan *Phishing*

Analisis terhadap kerentanan korban *phishing* dapat dipahami secara mendalam melalui kerangka Teori Aktivitas Rutin Cohen dan Felson, yang menekankan bahwa kejahatan terjadi ketika pelaku yang termotivasi bertemu dengan target yang sesuai di tengah absennya pengawasan yang memadai. Dalam konteks kejahatan *phishing* di Indonesia, ketiga elemen tersebut terpenuhi secara bersamaan akibat perubahan pola aktivitas digital masyarakat yang berlangsung sangat cepat namun tidak diimbangi dengan peningkatan literasi dan kewaspadaan digital yang setara.

Elemen pertama, yakni ketersediaan target yang sesuai (*suitable target*), sangat jelas terlihat dari tingginya intensitas aktivitas digital masyarakat Indonesia sehari-hari. Survei APJII 2025 mencatat bahwa delapan dari sepuluh penduduk Indonesia kini terhubung ke internet, namun sebanyak 41 persen pengguna bahkan tidak menyadari bahwa akun atau

perangkat mereka pernah mengalami masalah keamanan, sementara penggunaan langkah proteksi seperti *Two-Factor Authentication* dan VPN masih sangat minim (InternetSehat.id, 2025). Kondisi ini menciptakan jutaan target potensial yang setiap harinya aktif berinteraksi di ruang digital, memiliki akun keuangan bernilai tinggi, namun minim perlindungan. Modus *phishing giveaway* artis palsu di media sosial menjadi salah satu ilustrasi paling nyata dari fenomena ini. Pelaku mencatut nama artis ternama seperti Baim Wong, Ria Ricis, hingga Raffi Ahmad untuk memikat korban, sehingga korban yang sudah terpedaya biasanya dengan sukarela memberikan uang sebagai biaya administrasi karena tergiur oleh nilai hadiah palsu yang dijanjikan jauh lebih besar (Turnip, 2024). Korban dalam kasus ini adalah individu yang aktif menggunakan media sosial setiap hari, menjadikan mereka target yang sangat sesuai bagi pelaku yang memahami betul psikologi pengguna platform digital.

Elemen kedua, yakni ketiadaan pengawas yang cakap (*absence of capable guardian*), tercermin dari lemahnya kemampuan korban dalam memverifikasi keaslian informasi yang diterima sebelum mengambil tindakan. Pada 29 Maret 2024, saldo rekening nasabah BRI di Serang habis terkuras setelah ia menginstal APK berkedok "update BRImo" yang dikirim melalui WhatsApp, dengan pihak bank menegaskan korban harus menempuh proses hukum karena data rahasia sudah bocor (Wahyuningtias, 2025). Kasus ini memperlihatkan secara gamblang bagaimana ketiadaan *capable guardian* dalam diri korban, berupa ketidakmampuan mengenali tanda-tanda penipuan dan ketiadaan langkah verifikasi, menjadi celah yang langsung dimanfaatkan pelaku. Modus *phishing* semacam ini bekerja dengan mengirimkan pesan WhatsApp yang mengatasnamakan bank dengan tampilan yang tampak meyakinkan lengkap dengan logo bank dan bahasa resmi, serta satu tautan yang diminta untuk diklik, dan dalam hitungan menit setelah mengikuti instruksi tersebut saldo rekening korban bisa raib. Kecepatan dan kepanikan yang diciptakan pelaku inilah yang secara efektif melumpuhkan kemampuan korban untuk berpikir kritis dan melakukan verifikasi sebelum bertindak.

Secara struktural, kerentanan korban *phishing* di Indonesia juga diperkuat oleh fakta bahwa kerugian yang ditimbulkan terus membesar dari tahun ke tahun. Data Indonesia Anti-Scam Center OJK mengungkapkan bahwa total kerugian yang dilaporkan akibat kejahatan siber dalam periode November 2024 hingga November 2025 telah menembus Rp8,2 triliun (Andarningtyas, 2025). Angka yang sangat besar ini mencerminkan betapa masifnya jumlah korban yang jatuh setiap tahunnya, sekaligus menunjukkan bahwa kerentanan ini bukan sekadar persoalan individu yang ceroboh, melainkan merupakan persoalan struktural yang menyangkut rendahnya literasi digital masyarakat secara kolektif. Dengan demikian, Teori Aktivitas Rutin menegaskan bahwa upaya penurunan angka korban *phishing* tidak cukup hanya

dengan mengandalkan penegakan hukum terhadap pelaku, tetapi juga harus disertai dengan penguatan *capable guardian* di level individu maupun sistem, melalui peningkatan literasi digital, pengembangan teknologi keamanan yang lebih adaptif, serta penguatan regulasi perlindungan pengguna di ruang digital.

KESIMPULAN

Penelitian ini menegaskan bahwa fenomena penipuan *phishing* di Indonesia tidak dapat dipahami secara memadai hanya melalui pendekatan hukum dan teknis semata, melainkan membutuhkan analisis yang lebih komprehensif melalui perspektif sosiologi kriminalitas. Berdasarkan hasil kajian yang telah dilakukan, ditemukan bahwa kejahatan *phishing* merupakan produk dari interaksi kompleks antara tekanan struktural sosial, lemahnya ikatan sosial individu, proses pembelajaran kejahatan dalam komunitas digital, serta perubahan pola aktivitas masyarakat di era digital yang tidak diimbangi dengan kesiapan literasi dan keamanan yang memadai.

Dari sisi motif pelaku, Teori *Anomie* Merton menjelaskan bahwa sebagian pelaku *phishing* terdorong oleh ketimpangan antara tujuan finansial yang ditanamkan masyarakat dengan terbatasnya akses mereka terhadap sarana-sarana yang sah. Hal ini terbukti dari profil pelaku seperti mahasiswa muda dan lulusan SMK yang memiliki keahlian teknis tinggi namun tidak memiliki akses ke jalur ekonomi formal yang memadai, sehingga memilih kejahatan siber sebagai respons *innovation* atas tekanan struktural yang mereka hadapi. Teori Kontrol Sosial Hirschi memperkuat pemahaman ini dengan menunjukkan bahwa lemahnya ikatan sosial pelaku, yang tercermin dari cara mereka beroperasi secara anonim di balik anonimitas dunia digital tanpa merasa terikat oleh norma dan konsekuensi sosial, menjadi faktor penentu yang memungkinkan dorongan menyimpang tersebut terwujud menjadi tindakan nyata. Sementara itu, Teori *Differential Association* Sutherland menambahkan dimensi pembelajaran sosial, dalam kejahatan *phishing* tidak berhenti pada satu pelaku melainkan menyebar melalui jaringan digital yang menormalisasi dan mengkomersialisasikan teknik penipuan siber kepada individu-individu lain dalam ekosistem komunitas kejahatan yang terorganisir.

Dari sisi kerentanan korban, Teori Aktivitas Rutin Cohen dan Felson menjelaskan bahwa tingginya angka korban *phishing* di Indonesia merupakan konsekuensi dari pertemuan antara jutaan pengguna internet yang aktif bertransaksi digital sebagai target yang sesuai, dengan minimnya pengawasan baik berupa literasi digital, sistem keamanan aktif, maupun mekanisme verifikasi yang memadai. Perubahan aktivitas rutin masyarakat yang kini sangat

bergantung pada platform digital untuk berbagai keperluan sehari-hari secara tidak langsung telah memperluas ruang operasi pelaku *phishing*, menjadikan setiap pengguna yang tidak waspada sebagai target potensial yang mudah dijangkau.

Secara keseluruhan, penelitian ini memberikan kontribusi pemahaman bahwa penanggulangan kejahatan *phishing* yang efektif memerlukan pendekatan multi-dimensi. Tidak cukup hanya dengan memperketat regulasi hukum dan memperkuat sistem keamanan teknis, tetapi juga harus disertai dengan upaya memperkuat ikatan sosial masyarakat, meningkatkan literasi digital secara masif dan merata, serta memutus rantai pembelajaran kejahatan siber melalui pengawasan yang lebih ketat terhadap komunitas-komunitas digital yang menormalisasi perilaku kriminal. Dengan demikian, perspektif sosiologi kriminalitas terbukti memberikan kerangka analisis yang lebih kaya dan komprehensif dalam memahami akar sosial dari fenomena *phishing*, sekaligus membuka ruang bagi pendekatan pencegahan yang lebih holistik dan berkelanjutan.

DAFTAR PUSTAKA

Andarningtyas, N. (2025). *Ini Dia 3 Modus Penipuan Terbanyak, Jangan Sampai Tertipu!* ANTARA News. https://www.antaranews.com/berita/5299165/ini-dia-3-modus-penipuan-terbanyak-jangan-sampai-tertipu

Azis, L., & Ridwan. (2025). Dinamika Kriminalitas dalam Masyarakat: Faktor Sosial dan Solusinya. *Jurnal PKM Merah Putih*, *1*(1), 33–43. https://doi.org/10.65661/jpkmmp.v1i1.17

Butarbutar, J. M. (2025). Revolusi Digital dan Tantangan Kriminologis: Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi. *Media Hukum Indonesia (MHI)*, *2*(6), 145–150. https://doi.org/10.5281/zenodo.15493512

CNN Indonesia. (2024). *Serangan Phishing Meningkat 40 Persen Sepanjang 2023, Cek Targetnya*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20240313142500-192-1073789/serangan-phishing-meningkat-40-persen-sepanjang-2023-cek-targetnya

CNN Indonesia. (2024). *Undangan Pernikahan Palsu Masih Gentayangan, Cek Daftar APK Terbaru*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20240724163900-192-1125107/undangan-pernikahan-palsu-masih-gentayangan-cek-daftar-apk-terbaru

Dewi, N. K. R. K. (2025). Analisis Kritis Teori Kontrol Sosial dan Aplikasinya dalam Pencegahan Kejahatan Komunitas. *Jurnal Aktual Justice*, *10*(1), 79–83. https://doi.org/10.70358/aktualjustice.v10i1.1504

Farhansyah, A. (2025). *Mengatasi Ancaman Phishing di Era Digital: Tantangan dan Upaya di Indonesia*. KBR.Id. https://kbr.id/articles/ragam/mengatasi-ancaman-phishing-di-era-digital-tantangan-dan-upaya-di-indonesia

Habib, M. A. F., Ramadhani, M., Fatkhullah, M., Diniati, B. T. A., & Istiqoma, I. (2024). Strategi Digital Marketing atas Produk dan Layanan yang Ditawarkan dalam Bisnis Prostitusi Online. *Jurnal Iptekkom (Jurnal Ilmu Pengetahuan & Teknologi informasi)*, *26*(1), 53-78.

Ichsan, L. O. M. (2021). Kajian Sosiologi Kriminal terhadap Penanggulangan Cybercrime melalui Phising. *JURNAL DARUSSALAM: Pemikiran Hukum Tata Negara dan Perbandingan Mazhab*, *1*(1), 39–48. https://doi.org/10.59259/jd.v1i1.4

IDADX. (2023). *Laporan Aktifitas Phishing Domain.ID Periode Q1 2023*. https://api.idadx.id/documents/uploads/1689234933_Laporan%20Q1%202023.pdf.pdf

IDADX. (2025). *Laporan Aktivitas Abuse Domain .ID: Periode Q1 2025 Januari – Maret 2025*. https://api.idadx.id/documents/uploads/1745306450_Laporan%20Q1%202025.pdf.pdf

IDADX. (2026). *Laporan Aktivitas Abuse Domain .ID: Periode Q1 2026 Januari – Maret 2026*. https://api.idadx.id/documents/uploads/1776831567_Laporan%20Q1%202026%20Final.pdf.pdf

InternetSehat.id. (2025). *Lanskap Pengguna Internet Indonesia 2025: Koneksi Meluas, Literasi Masih Lemas*. InternetSehat.Id. https://internetsehat.id/2025/08/08/lanskap-pengguna-internet-indonesia-2025-koneksi-meluas-literasi-masih-lemas/

Iskandar, O. (2024). Analisis Kejahatan Online Phishing pada Masyarakat. *Leuser: Jurnal Hukum Nusantara*, *1*(2), 32–36. https://journal.myrepublikcorp.com/index.php/leuser/article/view/85

Maulida, K. (2025). Kriminalitas dan Hukum: Perspektif Sosiologi Terkait Kontrol Sosial dan Hukum. *Jurnal Hukum Caraka Justitia*, (1), 14–28. https://journal.myrepublikcorp.com/index.php/leuser/article/view/85

Mulyadi, Nurdin, A. A., Anjani, A. A., Fiqih, D. A., Firdha, S., Yudistio, M. A., Maulana, M. K., & Rabbani, R. A. A. (2024). Analisis Penipuan Online melalui Media Sosial dalam Perspektif Kriminologi. *Media Hukum Indonesia (MHI)*, *2*(2), 74–82. https://doi.org/10.5281/zenodo.11183088

Sahfitri, A., & Rosmalinda. (2024). Penipuan Digital melalui Tautan Phishing. *Jurnal Dialektika Hukum*, *6*(2), 92–107. https://ejournal.fisip.unjani.ac.id/index.php/jurnal-dialektika-hukum/article/view/2881

Tim detikcom. (2026). *6 Fakta Sejoli Sindikat Phishing Tools Internasional Dibongkar Bareskrim*. DetikNews. https://news.detik.com/berita/d-8457151/6-fakta-sejoli-sindikat-phishing-tools-internasional-dibongkar-bareskrim

Trianurahmah, A., Fauzi, A., Tyas, E. N., Suryanto, M. A., Rizky, M., & Wibisono, P. (2025). Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phising dengan Modus Berbasis Link. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, *1*(2), 74–88. https://doi.org/10.63217/orbit.v1i2.81

Turnip, W. M. (2024). *Sudah Banyak Korban Nih, Waspada Penipuan Modus Giveaway Catut Nama Artis*. Riau Online. https://www.riauonline.co.id/fact-check/read/2024/07/12/sudah-banyak-korban-nih-waspada-penipuan-modus-giveaway-catut-nama-artis

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

Wahyuningtias, N. A. (2025). Analis Normatif Perlindungan Hukum terhadap Korban Kejahatan Siber dalam Modus Phishing Rekening Bank di Indonesia. *Judge: Jurnal Hukum*, *6*(6), 1972–1983. https://doi.org/10.54209/judge.v6i06.1564