KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa (JIPM)
Vol.4, No.4 Agustus 2026
e-ISSN: 3025-5465, p-ISSN : 3025-7964, Hal 324-336
DOI : https://doi.org/10.61722/jipm.v4i4.2654

PENIPUAN MIKRO DI MEDIA SOSIAL (INSTAGRAM DAN X) PADA KALANGAN MAHASISWA

Ciek Julyati Hisyam, Ashfiya Salsabila, Ardelia Zahirah Rahman, Afifah Maharani, Nabilah Destin Amelia
Program Studi Pendidikan Sosiologi, Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Jakarta, Jl. Rawamangun Muka Raya, RT.11/RW.14, Rawamangun, Kec. Pulo Gadung,
Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta 13220
nabilahdestin@gmail.com

Abstract.*The rapid expansion of informal digital transactions on social media platforms has created a highly vulnerable ecosystem for cybercrimes targeting younger demographics. This study aims to analyze the phenomenon of micro-scamming among college students on Instagram and X (formerly Twitter) using Routine Activity Theory and Labeling Theory. Utilizing a qualitative descriptive approach, data were gathered through online text-based interviews and cyber documentation from four student informants who experienced financial losses ranging from Rp20,000 to Rp200,000. The findings indicate that micro-scamming manifests through the convergence of motivated offenders exploiting cyber-anonymity, suitable student targets, and the complete absence of capable transaction guardians. Furthermore, an under-reporting phenomenon occurs due to a pragmatic rational choice cost-benefit analysis by victims, as formal legal procedures outweigh the minor financial losses. Socially, a digital de-labeling process normalizes these crimes as mere "bad luck" or consumer negligence, shifting the security burden onto victims and allowing offenders to operate recurrently. Consequently, this continuous cycle of micro-scamming causes a systemic decline in digital social trust and fosters a culture of generalized distrust, which structurally disrupts the peer-to-peer informal economic network relied upon by students with limited purchasing power. These implications suggest that social media developers must implement AI-driven fraud detection mechanisms, and higher education institutions should integrate critical digital safety programs to rebuild a secure digital social capital.*

Keywords: *Cyber-Anonymity; De-Labeling; Digital Social Trust; Micro-Scamming; Under-Reporting.*

Abstrak.Pesatnya ekspansi transaksi digital informal di platform media sosial telah menciptakan ekosistem yang sangat rentan terhadap kejahatan siber yang menyasar demografi muda. Penelitian ini bertujuan untuk menganalisis fenomena penipuan mikro (*micro-scamming*) di kalangan mahasiswa pada platform Instagram dan X menggunakan Teori Aktivitas Rutin dan Teori Labeling. Dengan menggunakan pendekatan deskriptif kualitatif, data dihimpun melalui wawancara daring berbasis teks dan studi dokumentasi digital dari empat informan mahasiswa yang mengalami kerugian finansial berkisar antara Rp20.000 hingga Rp200.000. Hasil penelitian menunjukkan bahwa penipuan mikro bermanifestasi melalui konvergensi pelaku yang memanfaatkan anonimitas siber, target mahasiswa yangn sesuai, dan ketiadaan penjaga transaksi yang cakap secara total. Lebih lanjut, fenomena tidak melapor (*under-reporting*) terjadi karena kalkulasi pilihan rasional yang pragmatis oleh korban, di mana biaya prosedur hukum formal dirasa jauh melebihi nilai kerugian material yang kecil. Secara sosial, terjadi proses *de-labeling* digital yang menormalisasi kejahatan ini sebagai sekadar "nasib apes" atau kecerobohan konsumen, sehingga menggeser beban keamanan kepada korban dan memungkinkan pelaku beroperasi secara berulang. Konsekuensinya, siklus penipuan mikro yang berkelanjutan ini menyebabkan penurunan kepercayaan sosial digital secara sistemik dan menumbuhkan budaya ketidakpercayaan yang meluas (*generalized distrust*), yang secara struktural mengganggu jaringan ekonomi informal peer-to-peer yang diandalkan oleh mahasiswa dengan daya beli terbatas. Implikasi ini menunjukkan bahwa pengembang media sosial harus menerapkan mekanisme deteksi penipuan berbasis kecerdasan buatan, dan institusi pendidikan tinggi perlu mengintegrasikan program keamanan digital yang kritis guna membangun kembali modal sosial digital yang aman.

Kata Kunci: Anonimitas Siber; De-Labeling; Kepercayaan Sosial Digital; Penipuan Mikro; Tidak Melapor.

Naskah Masuk: 05 Juni 2026; Revisi: 10 Juni 2026; Diterima: 18 Juni 2026; Terbit: 23Juni 2026

PENDAHULUAN

Perkembangan teknologi digital telah mengubah pola konsumsi generasi muda secara fundamental dan menyeluruh. Indonesia sebagai salah satu negara dengan ekosistem digital terbesar di Asia Tenggara mencatat angka yang meng-impresif pada Januari 2025, tercatat sebanyak 143 juta identitas pengguna media sosial aktif, angka yang setara dengan 50,2 persen dari total populasi Indonesia[1]. Di antara kelompok pengguna paling aktif tersebut adalah mahasiswa generasi Z yang lahir dalam ekosistem digital dan tumbuh bersama perkembangan platform-platform media sosial. Bagi kelompok ini media sosial bukan sekadar ruang berkomunikasi, melainkan juga telah berevolusi menjadi pasar informal yang berdenyut setiap saat, tempat transaksi jual-beli, peminjaman jasa, dan pertukaran komoditas berlangsung tanpa batas waktu dan tanpa batas wilayah[2].

Budaya konsumerisme digital di kalangan mahasiswa telah melahirkan ekosistem perdagangan informal yang menggunakan platform-platform seperti Instagram (khususnya fitur *Direct Message*/DM) dan X (platform microblogging yang sebelumnya dikenal sebagai Twitter) sebagai medium utama. Berbagai jenis transaksi berlangsung di sini: pembelian akun layanan aplikasi premium bekas pakai (Netflix, Spotify Premium, Canva Pro, Capcut Pro, AI Pro) dengan harga lebih murah dari pasaran, pembelian produk *preloved* atau barang bekas layak pakai, pembelian tiket konser yang habis terjual di platform resmi dan kini diperdagangkan oleh *reseller* atau calo daring, hingga pembelian berbagai jasa digital seperti *boosting* followers, penulisan tugas, atau pembuatan desain grafis. Mayoritas transaksi ini dilakukan secara informal tanpa platform *marketplace* bersertifikat, tanpa sistem *escrow* (penitipan dana ke pihak ketiga), dan tanpa mekanisme

[1] DataReportal, Digital 2025: Indonesia (2025).

[2] Putra, R. A., Syaputri, I. K., & Muhsari, A. Y. (2026). Rebut Perhatian Gen Z! Newsjacking & E-WOM sebagai Cara Ampuh Perguruan Tinggi Rebut Perhatian Generasi Z. PT Kimhsafi Alung Cipta.

rekening bersama (rekber) yang biasa digunakan di marketplace-marketplace besar sebagai perlindungan bagi kedua pihak[3].

Kondisi ini berkorelasi langsung dengan tingkat literasi digital yang masih perlu ditingkatkan. Berdasarkan *Laporan Status Literasi Digital di Indonesia 2023* yang diterbitkan oleh Kementerian Komunikasi dan Informatika bersama Katadata Insight Center, indeks literasi digital nasional Indonesia berada pada angka 3,54 dari skala 5,0[4]. Meski menunjukkan peningkatan dari tahun-tahun sebelumnya, angka ini mengindikasikan bahwa kemampuan masyarakat termasuk mahasiswa dalam mengenali risiko dan ancaman di ekosistem digital belum sepenuhnya memadai untuk melindungi diri dari berbagai modus penipuan yang terus berevolusi. Keaktifan mahasiswa bertransaksi di media sosial yang tidak sebanding dengan kewaspadaan digital menciptakan kondisi yang rawan.

Kondisi ekosistem transaksi informal yang minim pengawasan inilah yang membuka celah lebar bagi berkembangnya fenomena penipuan mikro (*micro-scamming*). Penipuan mikro merujuk pada tindakan penipuan dalam transaksi daring dengan nominal kerugian yang relatif kecil dalam konteks Indonesia berkisar antara Rp20.000 hingga Rp200.000 per kejadian yang dilakukan melalui akun media sosial anonim atau semi-anonim. Meskipun nominal kerugian per kasus tergolong kecil frekuensi terjadinya sangat tinggi dan bersifat berulang. Data dari portal Patroli Siber Polri mencatat bahwa terdapat 14.496 laporan penipuan online yang masuk ke sistem mereka.

Keengganan melaporkan bukan semata cerminan dari sikap apatis atau pasrah melainkan merupakan buah dari kalkulasi rasional yang dilakukan oleh korban. Biaya yang harus dikeluarkan untuk melaporkan sebuah kasus kepada kepolisian berupa waktu, energi, dokumen administrasi, dan kemungkinan harus mengikuti proses hukum yang panjang dirasa jauh melampaui nilai material yang hilang. Seperti yang diamati oleh laporan Consumers International (2023) e-commerce scams dan impostor scams merupakan dua jenis penipuan yang paling marak di media sosial; dan dalam kedua kasus tersebut, "hampir mustahil bagi konsumen untuk mendapatkan kembali uang mereka karena mereka dianggap telah 'setuju' untuk menyerahkan uang secara sukarela[5].

Fenomena keengganan melaporkan ini memiliki dampak yang jauh lebih dalam dari sekadar kerugian material individual. Ketika penipuan dengan nominal kecil berulang kali terjadi tanpa ada sanksi bagi pelakunya maka secara bertahap dan sistemik ia menggerus kepercayaan sosial (*social trust*) di komunitas digital. Kepercayaan sosial adalah fondasi yang menopang semua transaksi ekonomi, baik formal maupun informal. Ia adalah keyakinan kolektif bahwa anggota komunitas lain akan bertindak sesuai norma dan tidak akan memanfaatkan kerentanan pihak lain secara oportunistik[6].

Berdasarkan uraian di atas, terdapat kesenjangan yang signifikan antara prevalensi penipuan mikro di media sosial yang sangat tinggi di kalangan mahasiswa dengan minimnya respons hukum dan akademis terhadap fenomena ini. Kajian sosiologis yang secara khusus membedah dinamika penipuan mikro mulai dari motivasi pelaku, keputusan *under-reporting* korban, proses *de-labeling* sosial, hingga dampaknya

---

[3] Kementerian Komunikasi dan Informatika & Katadata Insight Center, Status Literasi Digital di Indonesia 2023 (2023), hlm. 14–17.

[4] Ibid., indeks literasi digital 3,54 dari 5,0.

[5] Consumers International, Social Media Scams (2023), hlm. 7.

[6] Januraga, P. P., & Ked, S. (2024). Modal Sosial dalam Meningkatkan Kesehatan Masyarakat: Pendekatan Teoritis dan Empiris. Baswara Press.

terhadap *social trust* digital masih sangat terbatas dalam literatur akademis Indonesia. Oleh karena itu, fokus utama penelitian ini dirumuskan untuk mengkaji pola modus operandi penipuan mikro di Instagram dan X, mengidentifikasi faktor sosial-struktural yang mendorong *under-reporting*, serta membedah pengaruh mekanisme *de-labeling* terhadap penurunan kepercayaan sosial dalam komunitas digital mahasiswa.

Sejalan dengan rumusan tersebut, penelitian ini bertujuan untuk menganalisis secara mendalam fenomena penipuan mikro di media sosial Instagram dan X pada kalangan mahasiswa dengan memanfaatkan Teori Aktivitas Rutin (*Routine Activity Theory*) dan Teori Labeling (*Labeling Theory*) sebagai kerangka analisis utama. Secara spesifik, penelitian ini diarahkan untuk mendeskripsikan karakteristik penipuan siber skala mikro, mengurai faktor di balik keengganan melapor, serta menjelaskan proses normalisasi kejahatan bernominal kecil yang terjadi di lingkungan siber kampus.

Penelitian ini diharapkan dapat memberikan kontribusi teoritis yang berarti, khususnya dalam memperluas penerapan *Routine Activity Theory* dan *Labeling Theory* pada konteks kejahatan siber skala mikro melalui pengenalan konsep 'de-labeling digital'. Secara praktis, studi ini ditargetkan mampu meningkatkan literasi digital kritis mahasiswa, menyediakan dasar ilmiah bagi program *digital safety* di perguruan tinggi, serta memberikan data empiris bagi pembuat kebijakan (seperti Komdigi dan OJK) dan platform media sosial untuk membangun mekanisme pelaporan yang adaptif dan responsif bagi perlindungan konsumen.

KAJIAN TEORITIS

Kerangka analisis pertama yang digunakan untuk membedah ruang terjadinya kejahatan ini adalah Teori Aktivitas Rutin (*Routine Activity Theory*) yang diperkenalkan pertama kali oleh Lawrence E. Cohen dan Marcus K. Felson melalui artikel monumental mereka yang berjudul *"Social Change and Crime Rate Trends A Routine Activity Approach*", dipublikasikan dalam *American Sociological Review* Volume 44, Nomor 4, pada tahun 1979[7]. Artikel ini menjadi salah satu kontribusi paling berpengaruh dalam sejarah kriminologi modern menggeser paradigma analisis kejahatan dari fokus pada *siapa pelakunya* ke fokus pada *kondisi apa yang memungkinkan kejahatan terjadi*.

Argumen inti dari Cohen dan Felson adalah bahwa tindakan kejahatan predator (kejahatan yang melibatkan kontak langsung antara pelaku dan korban/objek) tidak dapat dipahami secara memadai hanya dengan menganalisis karakteristik individual pelaku. Sebaliknya, mereka menegaskan bahwa *"Most criminal acts require convergence in space and time of likely offenders, suitable targets and the absence of capable guardians against crime."* [8]. Dengan kata lain, kejahatan terjadi ketika dan di mana tiga elemen minimal bertemu secara bersamaan dalam satu ruang dan waktu, yaitu Pelaku yang Termotivasi (*Motivated Offender*), Target yang Sesuai (*Suitable Target*), Ketiadaan Penjaga yang Cakap (*Absence of Capable Guardians*).

Dalam konteks digital abad ke-21, aktivitas rutin mahasiswa telah bergeser secara masif ke platform *online* untuk berbelanja, mencari hiburan, dan bertransaksi informal. Pergeseran struktural ini meningkatkan frekuensi pertemuan antara pelaku yang memanfaatkan anonimitas siber, mahasiswa sebagai target yang sesuai karena memiliki

[7]Cohen, L.E. & Felson, M. (1979). "Social Change and Crime Rate Trends: A Routine Activity Approach." American Sociological Review, 44(4),

rutinitas konsumsi tinggi dengan daya beli terbatas, serta kondisi platform Instagram dan X yang minim sistem *escrow* atau *buyer protection* sehingga menciptakan ketiadaan penjaga yang cakap.

Selain melihat ruang kesempatan kejahatan melalui aktivitas rutin, dinamika pasca-kejahatan dan keberulangan tindakan pelaku dianalisis menggunakan Teori Labeling (*Labeling Theory*) yang dikembangkan oleh Edwin M. Lemert (1951) dan Howard S. Becker (1963). Teori ini menggeser fokus dari pertanyaan *"mengapa orang melakukan tindakan menyimpang?"* ke pertanyaan *"bagaimana suatu tindakan mendapatkan atau kehilangan label 'menyimpang' dalam masyarakat?"*.

Edwin M. Lemert, dalam karya seminarnya "*Social Pathology: A Systematic Approach to the Theory of Sociopathic Behavior*" (1951), memperkenalkan dikotomi konseptual yang sangat berpengaruh antara deviasi primer (*primary deviance*) dan deviasi sekunder (*secondary deviance*)[9]. Deviasi primer mengacu pada tindakan pelanggaran norma yang bersifat awal dan belum mendapat respons sosial yang signifikan pelakunya belum internalisasi identitas sebagai "devian" atau "kriminal." Sebaliknya deviasi sekunder terjadi ketika seseorang mendapat label sosial sebagai devian atas tindakannya, dan label tersebut kemudian terinternalisasi sehingga membentuk identitas dan perilaku selanjutnya[10].

Dalam konteks penipuan mikro modus ini memperlihatkan dinamika yang menarik ketika pelaku pertama kali melakukan penipuan mikro (deviasi primer), masyarakat dan korban merespons secara minimal atau bahkan tidak merespons sama sekali karena nilai kerugiannya kecil[11]. Tanpa respons sosial yang berarti, pelaku tidak mendapatkan label "kriminal" atas tindakannya. Justru sebaliknya, pelaku yang berhasil "lolos" tanpa konsekuensi cenderung akan mengulangi dan mengeskalasi tindakannya itulah mekanisme yang oleh Lemert disebut sebagai proses menuju deviasi sekunder, di mana kejahatan menjadi bagian dari pola perilaku yang sistematis.

Howard S. Becker dalam karya ikonisnya "*Outsiders: Studies in the Sociology of Deviance*" (1963) membawa *Labeling Theory* ke tingkat kedalaman yang lebih radikal. Becker berargumen bahwa devians bukanlah kualitas inheren dari suatu tindakan melainkan merupakan produk dari proses sosial pelabelan. Ia menulis dengan tegas[12]: *"Deviance is not a quality of the act the person commits, but rather a consequence of the application by others of rules and sanctions to an 'offender.' The deviant is one to whom that label has successfully been applied; deviant behavior is behavior that people so label."*[13].

Argumen Becker ini memiliki implikasi analitis yang sangat signifikan untuk memahami fenomena penipuan mikro. Jika devians bukan kualitas intrinsik dari tindakan,

---

[9]Lemert, E.M. (1951). Social Pathology: A Systematic Approach to the Theory of Sociopathic Behavior. New York: McGraw-Hill Book Company.

[10]Amry, A., & Novembri, S. (2021). Analisis Bentuk Labelling terhadap Mantan Narapidana Narkotika di Kelurahan Kampung Jawa, Kota Solok, Sumatera Barat. Deviance Jurnal Kriminologi, 5(2), 118-135.

[11]Guspriyoga, R. (2025). Analisis Kriminologi Dan Viktimologi Terhadap Tindak Pidana Penipuan Melalui Transaksi Online Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Doctoral dissertation, Magister Hukum, Universitas Islam Sumatera Utara).

[12]Becker, H.S. (1963). Outsiders: Studies in the Sociology of Deviance. New York: The Free Press

[13]Ibid., hlm. 9.

maka pertanyaan kuncinya menjadi *siapa yang berhak mendefinisikan sebuah tindakan sebagai kejahatan, dan apa yang terjadi ketika kemampuan mendefinisikan itu tidak digunakan?* Dalam kasus penipuan mikro, terjadi apa yang dapat disebut sebagai **"***de-labeling"* sebuah proses di mana tindakan yang secara normatif seharusnya dikategorikan sebagai kejahatan (penipuan) justru tidak mendapat label tersebut dari masyarakat. Korban menyebutnya "apes", teman-teman menyebutnya "risiko belanja online", dan komunitas digital menganggapnya sebagai hal yang sudah biasa. Dalam absennya pelabelan sosial sebagai "kejahatan serius", pelaku beroperasi dalam ruang yang hampir bebas dari konsekuensi sosial.

Proses *de-labeling* ini diperparah oleh absennya *moral entrepreneurs*, baik dari pihak kepolisian, platform media sosial, maupun komunitas itu sendiri yang secara aktif dan konsisten menyuarakan penegakan aturan terhadap pelaku penipuan skala kecil. Akibatnya, pelaku dapat terus beroperasi di ruang maya dengan bebas dari stigma negatif masyarakat.

Kepercayaan sosial (*social trust*) adalah fondasi dari semua bentuk pertukaran sosial dan ekonomi, termasuk transaksi di ekosistem digital. Dalam tradisi sosiologi, Putnam (1995) mendefinisikan kepercayaan sosial sebagai komponen inti dari modal sosial (*social capital*) jaringan, norma, dan kepercayaan yang memfasilitasi koordinasi dan kerja sama untuk keuntungan bersama[14]. Dalam konteks ekonomi digital Asia Tenggara *Tech for Good Institute* (2024) menegaskan bahwa kepercayaan merupakan aset kritis yang menentukan keberhasilan ekosistem transaksi digital. Penipuan mikro yang berulang tanpa sanksi secara bertahap mengikis kepercayaan sosial digital dalam komunitas mahasiswa. Proses erosi ini berjalan melalui dua mekanisme yaitu *generalisasi distrust* (ketidakpercayaan yang semula terfokus pada satu penipu menyebar menjadi ketidakpercayaan terhadap semua penjual di media sosial) dan normalisasi kewaspadaan defensif (mahasiswa menjadi *overly suspicious* bahkan terhadap penjual yang legitimate)[15]. Kedua mekanisme ini pada akhirnya menghambat aktivitas ekonomi informal yang sebenarnya memiliki nilai positif bagi mahasiswa dengan daya beli terbatas.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif analisis. Pendekatan kualitatif dipilih untuk memahami, mengeksplorasi, dan mendeskripsikan secara mendalam fenomena penipuan mikro (*micro-scamming*) berdasarkan sudut pandang, pengalaman emosional, dan penghayatan langsung dari para korban di lingkungan mahasiswa. Desain deskriptif analisis digunakan untuk menggambarkan secara sistematis pola modus operasi pelaku berdasarkan Teori Aktivitas Rutin, serta bagaimana konstruksi sosial *de-labeling* terbentuk di kalangan mahasiswa. Penelitian ini dilaksanakan selama dua bulan, yaitu pada bulan Juni hingga Juli 2026. Mengingat fenomena yang dikaji berada dalam ekosistem digital, maka lokasi penelitian ini tidak dibatasi oleh batas geografis kampus fisik tertentu, melainkan bertempat di ruang digital siber (*cyber space*), khususnya pada jaringan interaksi informal antarmahasiswa

---

[14]Putnam, R.D. (1995). "Bowling Alone: America's Declining Social Capital." Journal of Democracy, 6(1), 65–78.

[15]Apriyanto, W. P. (2025). Analisis kriminologi terhadap fenomena buzzer di media sosial dan dampaknya terhadap legitimasi media pers. Jurnal Sosial-Politika, 6(1), 1-12.

di platform media sosial Instagram (fitur *Direct Message*) dan X (fitur *Direct Message* dan *Menfess*).

Subjek penelitian atau informan dalam studi ini ditentukan dengan menggunakan teknik *purposive sampling*. Kriteria informan yang ditetapkan meliputi mahasiswa aktif yang sedang menempuh studi di perguruan tinggi, pengguna aktif media sosial Instagram dan/atau X, serta pernah menjadi korban penipuan mikro dalam transaksi informal (berupa jasa aplikasi premium, *merchandise photocard* K-Pop idol, layanan konversi pulsa *handphone*, atau *voucher* promo bioskop) dengan nominal kerugian antara Rp20.000 hingga Rp200.000 dalam kurun waktu satu tahun terakhir. Berdasarkan kriteria tersebut, diperoleh 4 orang informan mahasiswa yang bersedia membagikan pengalaman transaksinya secara sukarela. Profil mendalam mengenai para informan penelitian dapat dicermati pada Tabel 1.

Tabel 1. Profil Informan Penelitian

No	Nama/ Inisial	Usia	Status	Jenis Transaksi yang Ditipu	Nominal Kerugian	Platform Tempat Tertipu
1	Informan 1 (Y)	22 thn	Mahasiswa	Jasa Aplikasi Premium (Netflix)	Rp30.000	X (twitter)
2	Informan 2 (L)	20 thn	Mahasiswa	Merchandise Photocard (PC) K-Pop Idol	Rp21.000	X (twitter)
3	Informan 3 (A)	20 thn	Mahasiswa	Layanan Konversi Pulsa Handphone menjadi Saldo Rekening Bank	Rp50.000	Instagram
4	Informan 4 (N)	20 thn	Mahasiswa	Voucher Promo Bioskop (Buy 1 Get 1)	Rp53.000	X (twitter)

Sumber: Data Primer Diolah Kelompok (2026)

Teknik pengumpulan data dalam penelitian ini bertumpu pada dua metode utama, yaitu wawancara daring berbasis teks (*online text-based interview*) dan studi dokumentasi digital (*cyber documentation*). Proses wawancara dilakukan secara daring dengan memanfaatkan fitur pesan teks pada aplikasi WhatsApp, Instagram DM, atau X DM. Metode berbasis teks ini dipilih secara sadar demi kenyamanan psikologis informan, mengingat korban penipuan mikro sering kali merasa malu atau enggan bercerita secara lisan. Melalui ketikan teks, informan memiliki waktu yang fleksibel untuk merefleksikan kembali ingatan kronologis mereka secara santai dan jujur tanpa tekanan emosional langsung. Sementara itu, studi dokumentasi digital dilakukan dengan mengumpulkan rekam jejak digital otentik yang disediakan oleh informan, yang meliputi tangkapan layar

(*screenshot*) ruang obrolan penipuan, profil akun pelaku, testimoni palsu yang digunakan pelaku, serta bukti transfer digital berupa *m-banking* atau *e-wallet*.

Seluruh data yang terkumpul kemudian diolah menggunakan metode analisis deskriptif kualitatif yang mengadopsi model interaktif dari Miles, Huberman, dan Saldaña. Operasionalisasi model ini dijalankan melalui tiga alur aktivitas simultan: (1) kondensasi data (*data condensation*), di mana peneliti melakukan seleksi, pemfokusan, dan transformasi tajam terhadap transkrip wawancara tekstual agar mengerucut pada esensi pemikiran korban; (2) penyajian data (*data display*), berupa pengorganisasian informasi ke dalam matriks profil teoretis dan narasi deskriptif yang memetakan keterkaitan antar-variabel tindakan; serta (3) penarikan maupun verifikasi kesimpulan (*conclusion drawing/verification*), yang melingkupi proses pemaknaan pola-pola keteraturan sejak awal pengumpulan data guna menguji validitas tafsir teoretis yang dibangun.

HASIL DAN PEMBAHASAN

A. Pola dan Modus Operandi Penipuan Mikro di di Instagram dan X

Fenomena penipuan mikro (*micro-scamming*) yang marak terjadi di platform Instagram dan X pada kalangan mahasiswa menunjukkan adanya transformasi struktural dalam pola kejahatan siber. Berdasarkan Teori Aktivitas Rutin (*Routine Activity Theory*) yang digagas oleh Cohen dan Felson (1979), tindakan kriminal di ruang siber ini bermanifestasi melalui konvergensi spasial dan temporal dari tiga elemen utama: *motivated offender* (pelaku yang termotivasi), *suitable target* (target yang sesuai), dan *absence of capable guardians* (ketiadaan penjaga yang cakap).

Pelaku (*motivated offender*) dalam ekosistem ini mengeksploitasi fitur anonimitas siber (*cyber-anonymity*) untuk mereplikasi identitas palsu tanpa risiko hukum yang berarti. Investigasi virtual para informan membuktikan adanya taktik multi-akun, di mana satu operator mengendalikan akun bodong seperti @_mopchi, @juiydoll, @barebIiss, dan @urswanly secara simultan. Karakteristik target yang sesuai (*suitable target*) pada kalangan mahasiswa dianalisis melalui empat properti VIVA (*Value, Inertia, Visibility, Accessibility*)

- ***Value*** **(Nilai):** Komoditas ekonomi yang ditawarkan memiliki nilai kebutuhan tinggi bagi gaya hidup mahasiswa, seperti akun aplikasi premium murah (Netflix), *merchandise* K-Pop langka, konversi pulsa menjadi uang tunai, dan *voucher* promo bioskop *Buy 1 Get 1*
- ***Inertia*** **(Inersia):** Transaksi digital memiliki inersia fisik yang nol karena pemindahan aset dilakukan secara instan menggunakan infrastruktur *e-wallet* atau QRIS (seperti ShopeePay atau bank digital).
- ***Visibility*** **(Visibilitas):** Kebutuhan mahasiswa terekspos secara transparan melalui *menfess*, tagar komunitas, atau algoritma pencarian media sosial.
- ***Accessibility*** **(Aksesibilitas):** Jalur komunikasi interaksi informal via Instagram DM dan X DM sangat mudah diakses tanpa memerlukan verifikasi identitas resmi.

Kondisi ini diperparah oleh ketiadaan pengawas yang mumpuni (*absence of capable guardians*). Berbeda dengan platform *marketplace* resmi yang memiliki sistem *escrow* (rekening bersama) atau mekanisme *buyer protection*, pasar informal di Instagram dan X beroperasi dalam ruang hampa regulasi. Pelaku secara taktis memanipulasi

psikologis korban melalui dua modus utama. Pertama, memanipulasi kesan (*impression*

management) dengan menyajikan testimoni Google Drive palsu atau memberikan fungsionalitas akun yang normal di awal transaksi sebelum melakukan pemblokiran sepihak. Kedua, manipulasi urgensi (*false urgency*) dengan skema *first pay, first get* guna memicu kepanikan dan perilaku irasional akibat takut kehilangan kesempatan (*Fear of Missing Out* / FOMO).

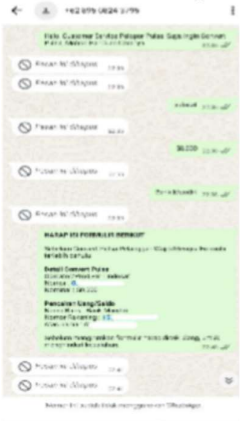
Gambar 1. Modus Umpan Ekonomi Lewat Promo di Platform X.

Sumber: Dokumentasi Kelompok (2026).

Gambar 2. Manipulasi Psikologis Urgensi Semu (*False Urgency*) via Chat.

Sumber: Dokumentasi Kelompok (2026).

Gambar 3. Administrasi Semu Guna Membangun Kredibilitas Layanan Jasa.



Sumber: Dokumentasi Kelompok (2026).

Gambar 4. Social Proof Palsu Berupa Tautan Testi Google Drive.

Sumber: Dokumentasi Kelompok (2026).

B. Analisis di Balik Tindakan Tidak Melapor (*Under-Reporting*) pada Korban

Meskipun frekuensi terjadinya penipuan mikro di kalangan mahasiswa sangat tinggi, mayoritas kasus berakhir tanpa adanya pelaporan ke pihak berwajib (*under-reporting*). Fenomena keengganan melapor ini bukanlah cerminan dari sikap apatis yang irasional, melainkan hasil dari kalkulasi pilihan rasional (*rational choice theory*) yang mendalam di pihak korban. Berdasarkan data empiris, nominal kerugian finansial yang dialami oleh para informan tergolong kecil dan "nanggung", yaitu berkisar antara Rp21.000 hingga Rp53.000 per kejadian.

Korban melakukan penimbangan biaya-manfaat (*cost-benefit analysis*) yang pragmatis. Biaya non-material yang harus dikeluarkan untuk memproses laporan secara hukum formal berupa alokasi waktu kuliah yang tersita, energi psikologis, dokumen administrasi, hingga stigma sosial dirasa jauh melampaui nilai material yang hilang. Hal ini dipertegas oleh narasi Informan 1 (Y) dan Informan 2 (L) berikut:

> *"aku sendiri dan korban lainnya males kak untuk melaporkan sampai ke pihak polisi karena kita tau sendiri kinerja polisi tidak akan membuat hasil duit kembali. Cuma buang-buang waktu aja kalau ngelapor"* (Wawancara daring dengan Informan 1, Juni 2026).

> *"Kalau gue pribadi sih karena ketipunya cuma 20k jadi cuma gue anggap angin lalu aja... kasus scammer di twt tuh jarang banget yang bisa nyampe ke meja hijau, ujung-ujungnya cuma nge spill akun... ganjaran yang diberi gak sepadan aja"* (Wawancara daring dengan Informan 2, Juni 2026).

Pernyataan di atas mengonfirmasi adanya ketidakpercayaan yang terstruktur (*structural distrust*) terhadap institusi penegak hukum dalam menangani kejahatan siber skala mikro. Realitas ini juga dialami oleh Informan 3 (A) dan Informan 4 (N), di mana setelah mereka mentransfer sejumlah dana atau pulsa, komunikasi langsung diputus secara sepihak (*ghosting*). Korban mengalami kelelahan psikologis akibat lingkaran setan janji garansi semu (*loophole warranty scam*) yang sengaja diulur oleh pelaku untuk menguras energi emosional korban hingga akhirnya menyerah secara sukarela. Celah kerugian yang kecil inilah yang dimanfaatkan pelaku sebagai tameng pelindung dari jerat pidana karena aparat penegak hukum cenderung memprioritaskan kasus dengan skala kerugian makro.

C. Mekanisme "De-Labeling" Digital dan Normalisasi Kejahatan

Teori Labeling dari Edwin M. Lemert (1951) dan Howard S. Becker (1963) menegaskan bahwa penyimpangan atau kejahatan bukanlah kualitas intrinsik dari suatu tindakan, melainkan konsekuensi dari proses pelabelan dan penerapan sanksi sosial oleh masyarakat. Namun, dalam konteks penipuan mikro di komunitas digital mahasiswa, terjadi sebuah anomali sosiologis yang disebut sebagai de-labeling digital. *De-labeling* merupakan sebuah proses di mana tindakan yang secara hukum memenuhi unsur pidana (penipuan) justru mengalami pengikisan label kriminalnya dan direduksi menjadi sekadar "nasib apes", "risiko belanja daring", atau "kecerobohan konsumen".

Proses penormalan ini terjadi karena lingkaran sosial terdekat korban sering kali melakukan tindakan menyalahkan korban secara halus (*subtle victim-blaming*). Bukannya melabeli pelaku sebagai penjahat siber yang amoral, fokus pembahasan digeser pada kurangnya kewaspadaan korban dalam membaca struktur harga pasar. Kondisi ini tergambar melalui pengakuan Informan 1 (Y) dan Informan 2 (L):

> *"sebenarnya bukan berarti yang lain menyalahkan, tetapi lebih ke memberitahu bahwa harga yang tertera ternyata sangat jauh dari harga pasar yang aku tidak tahu"* (Wawancara daring dengan Informan 1, Juni 2026).

> *"DUH gue ngerasanya cuma karena lagi apes doang lagi. Menurut gue sih emang harusnya kita yang lebih aware dalam berbelanja apalagi di dunia online... jadi ya kita yang harus jaga diri supaya gak terjerumus (sedih sebenernya malah kita yang disuruh aware, bukannya menghakimi pelaku tapi ya that's how our societies work"* (Wawancara daring dengan Informan 2, Juni 2026).

Absennya agen penggerak aturan (*moral entrepreneurs*) yang vokal untuk memburu pelaku tingkat mikro melahirkan konsekuensi pada keberulangan kejahatan (*sustainability of crime*). Akibat hukum formal lumpuh dan pelabelan negatif secara sosial menghilang, pelaku dapat leluasa melakukan deviasi primer secara berulang tanpa takut terkena stigma permanen. Sebagai mekanisme pertahanan alternatif, mahasiswa mengambil alih kontrol sosial dengan menciptakan sanksi sosial komunal mandiri berupa pembuatan *threads* eksposur atau *spill* akun pelaku di ruang siber X. Namun, efektivitas kontrol informal ini sangat lemah; pelaku cukup menghapus atau mengganti nama pengguna (*username*) mereka untuk membersihkan jejak digital, lalu kembali menjerat korban baru dalam ekosistem siber yang permisif.

D. Penurunan Kepercayaan Sosial Digital (*Digital Social Trust*) Mahasiswa

Dampak kumulatif dari maraknya penipuan mikro yang ternormalisasi ini membawa implikasi sosiologis yang destruktif terhadap modal sosial (*social capital*) generasi muda. Robert Putnam (1995) mendefinisikan kepercayaan sosial (*social trust*) sebagai inti dari modal sosial yang memfasilitasi koordinasi dan kerjasama demi keuntungan bersama. Ketika pasar informal di media sosial dipenuhi oleh tindakan manipulasi yang bebas dari sanksi, fondasi kepercayaan tersebut mengalami keruntuhan sistemik.

Erosi modal sosial ini berjalan melalui dua mekanisme utama:

- ***Generalized Distrust* (Ketidakpercayaan yang Meluas):** Rasa curiga mahasiswa tidak lagi hanya tertuju pada satu akun penipu spesifik, melainkan meluas menjadi skeptisisme radikal terhadap seluruh aktivitas transaksi ekonomi peer-to-peer di

Instagram dan X. Mahasiswa menjadi sangat curiga bahkan terhadap akun penjual jujur milik sesama mahasiswa yang sah (*legitimate*).

- **Normalisasi Kewaspadaan Defensif (*Defensive Vigilance*):** Komunitas mahasiswa dipaksa membangun benteng kecurigaan ekstra dalam setiap interaksi digital. Saling percaya yang semula menjadi instrumen efisiensi transaksi ekonomi kini digantikan oleh ketakutan komunal akan eksploitasi oportunistik.

Ketidakberdayaan struktur hukum di dunia nyata akhirnya memaksa korban menggunakan struktur moralitas tradisional sebagai senjata terakhir mereka. Hal ini tercermin dari perilaku Informan 4 (N) yang meluapkan krisis kepercayaannya dengan mengirimkan rentetan kutipan ayat suci serta ancaman hukum karma metafisika kepada nomor WhatsApp pelaku sebelum diblokir secara permanen. Pembiaran terhadap penipuan mikro pada akhirnya merusak ekosistem modal sosial digital yang mandiri. Jaringan ekonomi informal peer-to-peer yang seharusnya menjadi katup penyelamat bagi mahasiswa berdaya beli terbatas menjadi terhambat dan hancur akibat hilangnya rasa aman di ruang siber.

KESIMPULAN DAN SARAN

Kesimpulan dari penelitian ini menunjukkan bahwa fenomena penipuan mikro (*micro-scamming*) di kalangan mahasiswa melalui platform Instagram dan X merupakan implikasi nyata dari pergeseran aktivitas rutin masyarakat ke ruang siber yang tidak diimbangi oleh sistem pengawasan digital yang cakap. Konvergensi antara pelaku yang termotivasi oleh anonimitas siber, target mahasiswa yang rentan akibat pola konsumsi gaya hidup, serta ketiadaan sistem penjamin transaksi pihak ketiga menjadi stimulan utama terjadinya kejahatan ini. Sikap tidak melapor (*under-reporting*) yang masif di kalangan korban merupakan hasil kalkulasi pilihan rasional yang pragmatis, di mana kerugian material bernominal kecil (Rp21.000–Rp53.000) dirasa tidak sebanding dengan tingginya biaya non-material serta birokrasi hukum formal yang harus dihadapi. Lebih jauh, terjadi proses *de-labeling digital* di mana sosiokultural mahasiswa cenderung menormalisasi kejahatan ini sebagai sekadar nasib apes atau kecerobohan konsumen, yang pada akhirnya memberikan ruang aman bagi pelaku untuk mengulangi tindakannya secara berkelanjutan. Dampak paling destruktif dari fenomena ini adalah terjadinya penurunan kepercayaan sosial digital (*digital social trust*) secara sistemik yang memicu meluasnya budaya ketidakpercayaan komunal (*generalized distrust*) sehingga menghambat dan merusak jaringan ekosistem ekonomi informal peer-to-peer yang mandiri di kalangan generasi muda.

Berdasarkan kesimpulan tersebut, disarankan beberapa rekomendasi tindakan nyata bagi para pemangku kepentingan. Bagi mahasiswa, diperlukan peningkatan literasi digital kritis dan penguatan budaya defensif kolektif dengan cara selalu mengutamakan penggunaan rekening bersama (rekber) terpercaya atau platform pihak ketiga yang legal dalam setiap transaksi informal di media sosial. Bagi institusi perguruan tinggi, disarankan untuk menyelenggarakan program edukasi keamanan siber (*cyber-safety*) yang terintegrasi guna membangun kesadaran komunal mahasiswa terhadap berbagai modus penipuan daring yang terus berevolusi. Selain itu, bagi pengembang platform media sosial seperti Instagram dan X, studi ini memberikan rekomendasi kuat untuk merancang sistem pelaporan berbasis kecerdasan buatan yang lebih adaptif, cepat, dan responsif dalam mendeteksi kloning akun komersial anonim yang terindikasi menggunakan satu nomor kontak atau QRIS pembayaran yang sama agar dapat

memberikan efek jera yang nyata. Keterbatasan penelitian ini terletak pada fokus subjek yang terbatas pada lingkungan mahasiswa dengan nominal kerugian skala mikro di dua media sosial, sehingga direkomendasikan bagi peneliti yang akan datang untuk memperluas lokus penelitian pada ekosistem digital yang lebih luas serta melibatkan analisis viktimologi dari berbagai latar belakang kelas sosial masyarakat yang bervariasi.

DAFTAR REFERENSI

Amry, A., & Novembri, S. (2021). Analisis Bentuk Labelling terhadap Mantan Narapidana Narkotika di Kelurahan Kampung Jawa, Kota Solok, Sumatera Barat. *Deviance Jurnal Kriminologi*, 5(2), 118-135.

Apriyanto, W. P. (2025). Analisis kriminologi terhadap fenomena buzzer di media sosial dan dampaknya terhadap legitimasi media pers. *Jurnal Sosial-Politika*, 6(1), 1-12.

Becker, H. S. (1963). *Outsiders: Studies in the Sociology of Deviance*. New York: The Free Press. Diakses dari https://archive.org/details/outsidersstudies00beck

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588–608. https://doi.org/10.2307/2094589

Consumers International. (2023). *Social media scams*. London: Consumers International. Diakses dari https://www.consumersinternational.org/media/604472/social-media-scams-final-245.pdf

DataReportal. (2025). *Digital 2025: Indonesia*. Diakses dari https://datareportal.com/reports/digital-2025-indonesia

Guspriyoga, R. (2025). *Analisis Kriminologi Dan Viktimologi Terhadap Tindak Pidana Penipuan Melalui Transaksi Online Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik* (Disertasi Doktoral, Magister Hukum, Universitas Islam Sumatera Utara, Medan, Indonesia).

Januraga, P. P., & Ked, S. (2024). *Modal Sosial dalam Meningkatkan Kesehatan Masyarakat: Pendekatan Teoritis dan Empiris*. Denpasar: Baswara Press.

Kementerian Komunikasi dan Informatika & Katadata Insight Center. (2023). *Status Literasi Digital di Indonesia 2023*. Jakarta: Kemenkominfo. Diakses dari https://cdn1.katadata.co.id/media/Report_LITDIG_2023.pdf

Lemert, E. M. (1951). *Social Pathology: A Systematic Approach to the Theory of Sociopathic Behavior*. New York: McGraw-Hill Book Company. Diakses dari https://archive.org/details/socialpathologys00leme

Miles, M. B., Huberman, A. M., dan Saldaña, J. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. Sage Publications.

Putnam, R. D. (1995). Bowling alone: America's declining social capital. *Journal of Democracy*, 6(1), 65–78. https://doi.org/10.1353/jod.1995.0002

Putra, R. A., Syaputri, I. K., & Muhsari, A. Y. (2026). *Rebut Perhatian Gen Z! Newsjacking & E-WOM sebagai Cara Ampuh Perguruan Tinggi Rebut Perhatian*

Generasi Z. Jakarta: PT Kimhsafi Alung Cipta.