

The Dilemma of Paid Verified Account: Studi Psikologi terhadap Korban Spoofing dalam X dan Telegram

Tegar Adji Putra Pamungkas¹, Adinda Zidna Fauzateni², Putri Ambar Sari³, dan Afriza Animawan Arifin⁴

*Program Studi Psikologi, Fakultas Psikologi, Universitas Muhammadiyah Surakarta
tegaraadji@gmail.com*

Abstrak

Perubahan kebijakan verifikasi akun berbayar di media sosial, seperti X dan Telegram, telah menggeser makna tanda centang biru dari simbol keaslian menjadi atribut yang dapat dibeli secara bebas. Pergeseran ini memunculkan dinamika psikologis baru, di mana pengguna cenderung mempercayai akun bercentang biru tanpa mempertimbangkan validitas identitas pemiliknya. Penelitian ini bertujuan untuk memahami bagaimana fitur *verified account* berbayar memengaruhi pembentukan persepsi kepercayaan korban terhadap pelaku *spoofing* di media sosial. Penelitian ini menggunakan pendekatan kualitatif fenomenologis dengan melibatkan empat partisipan yang pernah menjadi korban penipuan oleh akun bercentang biru di X dan Telegram. Data dikumpulkan melalui wawancara semi-terstruktur dan dianalisis menggunakan *Interpretative Phenomenological Analysis (IPA)*. Hasil penelitian mengidentifikasi tiga tema utama, yaitu: (1) merasa aman melalui simbol digital, yang mencerminkan *trust bias* terhadap simbol digital; (2) profesionalitas semu sebagai dasar kepercayaan, yang ditunjukkan melalui pola komunikasi yang meyakinkan dan *social proof* yang dimanipulasi; serta (3) ilusi dalam pengambilan keputusan, yang berkaitan dengan kondisi internal korban seperti rasa aman berlebih (*false sense of security*). Temuan ini menunjukkan bahwa tanda centang biru berfungsi sebagai *false trust cue* yang memengaruhi mekanisme penilaian sosial secara intuitif. Secara praktis, penelitian ini menekankan pentingnya peningkatan literasi psikologis dan digital pengguna agar lebih kritis di dunia maya, serta memberikan implikasi bagi platform media sosial untuk merancang sistem verifikasi yang lebih transparan guna meminimalkan risiko penipuan berbasis manipulasi identitas.

Kata kunci: bias kepercayaan; fitur verifikasi berbayar; spoofing.

Abstract

The shift toward paid account verification policies on social media platforms such as X and Telegram has transformed the meaning of the blue checkmark from a symbol of authenticity into a purchasable attribute. This shift has introduced new psychological dynamics, wherein users tend to trust accounts with a blue checkmark without critically evaluating the validity of the account holder's identity. This study aims to examine how paid verified account features influence the formation of victims' trust perceptions toward spoofing perpetrators on social media. Employing a qualitative phenomenological approach, this research involved four participants who had experienced fraud committed by blue-checkmarked accounts on X and Telegram. Data were collected through semi-structured interviews and analyzed using Interpretative Phenomenological Analysis (IPA). The findings reveal three main themes: (1) a sense of security derived from digital symbols, reflecting a trust bias toward such markers; (2) perceived professionalism as a basis for trust, demonstrated through convincing communication patterns and manipulated social proof; and (3) illusion in decision-making, associated with internal conditions such as an excessive sense of security (false sense of security). These results indicate that the blue checkmark functions as a false trust cue that influences intuitive social judgment mechanisms. Practically, this study highlights the importance of enhancing users' psychological and digital literacy to foster more critical engagement in online environments. It also suggests implications for social media platforms to design more transparent verification systems in order to minimize the risk of identity-based fraud.

Keywords: spoofing; trust bias; paid verified feature.

LATAR BELAKANG

Fitur *verified account* merupakan simbol autentikasi yang menandakan bahwa suatu akun media sosial telah diverifikasi keasliannya oleh penyedia platform. Umumnya, akun yang telah diverifikasi dapat dikenali melalui adanya lencana biru atau tanda centang di sebelah nama pengguna sebagai penanda keaslian. Pada awalnya, lencana biru ini diberikan secara terbatas hanya kepada figur publik, lembaga resmi, atau tokoh terkenal dengan tujuan untuk membedakan dari akun palsu yang menyerupainya. Namun, sekitar akhir tahun 2022, terjadi perubahan kebijakan yang signifikan ketika platform X (sebelumnya dikenal sebagai Twitter) mulai memungkinkan seluruh penggunanya untuk memperoleh atau membeli lencana tersebut secara bebas. Kebijakan ini kemudian diikuti oleh berbagai platform media sosial lain seperti Telegram.

Dengan biaya berlangganan yang relatif terjangkau fitur *verified account* berbayar kini dapat diakses oleh pengguna dari berbagai lapisan sosial. Fenomena ini menunjukkan bahwa lencana biru tidak lagi menjadi sesuatu yang eksklusif yang hanya dimiliki oleh tokoh atau institusi tertentu saja, melainkan juga tersedia secara komersial. Laporan menunjukkan bahwa perubahan sistem verifikasi tersebut telah memicu kebingungan tentang makna lencana sebagai penanda kredibilitas di berbagai media sosial (Xiao et al., 2023). Menurut laporan media teknologi TechCrunch, terdapat lebih dari 1.4 juta pengguna X yang telah membeli fitur ini, sementara pengguna Telegram Premium telah mencapai lebih dari 12 juta pelanggan aktif hingga Desember 2024 (Mehta, 2024; Perez, 2024). Jumlah pelanggan dari fitur *verified account* berbayar ini diperkirakan akan terus bertambah seiring waktu. Angka ini menunjukkan bahwa *verified account* berbayar telah menjadi fenomena sosial baru dalam interaksi digital.

Meskipun demikian, perubahan sistem verifikasi ini justru menimbulkan konsekuensi yang tidak diantisipasi sebelumnya. Ketika simbol “centang biru” yang awalnya merepresentasikan kredibilitas kini dapat dibeli, makna simbol tersebut seharusnya ikut bergeser dan tidak lagi menjadi jaminan bahwa suatu akun yang memilikinya benar-benar kredibel. Namun, dalam praktiknya, banyak pengguna masih mempertahankan persepsi lama dengan menganggap bahwa akun bercentang biru sudah pasti lebih terpercaya dibandingkan akun biasa. Hal ini menunjukkan bahwa pemahaman pengguna belum banyak menyesuaikan diri dengan perubahan sistem yang terjadi. Akibatnya, kondisi ini kemudian membuka peluang baru bagi pelaku kejahatan siber untuk memanfaatkan kesempatan tersebut melalui praktik *spoofing*, yaitu penipuan dengan menyamar sebagai akun resmi atau *official* guna menyesatkan korbannya.

Kasus-kasus penipuan yang memanfaatkan *verified account* berbayar semakin sering muncul di berbagai platform media sosial. Laporan Federal Trade Commission menunjukkan bahwa *impersonation scam* merupakan salah satu bentuk penipuan yang paling banyak dilaporkan, dengan lebih dari 330.000 laporan penyamaran sebagai institusi atau bisnis pada tahun 2023 dan kerugian korban mencapai hampir 2,95 miliar dolar pada tahun 2024 (Federal Trade Commission, 2024, 2025). Fenomena ini tidak hanya terjadi pada skala institusional besar tersebut saja, tetapi juga terdapat dalam pengalaman individual di media sosial X dan Telegram. Misalnya, salah satu korban berinisial SP tertipu di platform X oleh akun yang menyamar sebagai toko resmi, sedangkan korban lain berinisial IR mengalami kejadian serupa di Telegram. Kedua korban mengaku tidak menaruh curiga karena pelaku memiliki tanda centang biru yang mereka asosiasikan dengan status keaslian dan kepercayaan. Temuan ini menunjukkan bahwa centang biru tidak hanya berfungsi sebagai fitur teknis saja, tetapi juga membentuk ekspektasi psikologis dari para pengguna di media sosial.

Fenomena tersebut menunjukkan adanya *trust bias*, dengan kecenderungan untuk langsung percaya pada tanda atau simbol yang terlihat resmi tanpa melakukan verifikasi lebih lanjut terhadap identitas dari akun tersebut. Selain itu, terdapat juga *halo effect*, dengan kecenderungan menilai kredibilitas secara keseluruhan hanya dari satu atribut yang menonjol, seperti tampilan, jumlah pengikut, atau penggunaan simbol centang biru berbayar ini. Dalam konteks ini, *trust bias* menjelaskan kecenderungan korban untuk langsung mempercayai akun tanpa mengecek validitasnya, sehingga kondisi ini dimanfaatkan dalam praktik *spoofing*, di mana pelaku menyamar sebagai pihak yang tampak kredibel untuk memperoleh kepercayaan dari korban tersebut. Sementara itu, *halo effect* memperkuat kesan pertama korban saat melihat tanda centang biru yang selama ini diasosiasikan dengan kredibilitas akun. Akibatnya, ketika satu aspek tersebut saja sudah terlihat cukup meyakinkan, korban cenderung menganggap seluruh informasi dari akun tersebut juga dapat dipercaya. Dengan demikian, *trust bias* dan *halo effect* berperan penting dalam membentuk keyakinan seseorang terhadap kredibilitas suatu sumber (Hoffner & Bond, 2022; Kahneman, 2011; Mayer et al., 1995; Thorndike, 1920).

Di Indonesia sendiri, penelitian menunjukkan bahwa persepsi terhadap kredibilitas akun di media sosial merupakan faktor penting yang memengaruhi kepercayaan pengguna terhadap informasi yang disajikan olehnya (Sa'diyah, 2020). Seseorang cenderung cepat menilai keaslian akun berdasarkan tampilan luar, seperti simbol dan jumlah pengikut, daripada meninjau fakta yang sebenarnya. Selain itu, penelitian lainnya mengutarakan bahwa kepercayaan dan karakteristik akun di media sosial memengaruhi intensi partisipasi dari para pengguna lain (Hartini & Hanafi, 2021). Pola ini menunjukkan bahwa kepercayaan digital kini lebih banyak dipengaruhi oleh aspek emosional yang bersifat *heuristik*, yaitu penilaian cepat sebagai jalan pintas kognitif dalam mengambil keputusan tanpa melalui evaluasi secara mendalam (Kahneman, 2011). Dalam media sosial, simbol seperti tanda centang biru dapat berfungsi sebagai *heuristic cue* yang memberikan kesan kredibel secara instan dan cepat, sehingga pengguna cenderung mengasosiasikan simbol tersebut dengan keaslian dan kepercayaan meskipun tidak selalu mencerminkan identitas yang sebenarnya. Kondisi ini pada akhirnya dapat meningkatkan risiko kesalahan penilaian, terutama ketika pengguna terlalu mengandalkan kesan awal dibandingkan verifikasi informasi yang lebih akurat.

Bagi korban *spoofing*, pengalaman tertipu oleh akun bercentang biru tidak hanya berdampak secara finansial, tetapi juga berpotensi menimbulkan konsekuensi psikologis. Korban dapat mengalami perasaan malu, marah, kecewa, serta kecenderungan menyalahkan diri sendiri karena merasa gagal bersikap kritis. Dalam jangka panjang, pengalaman ini dapat memengaruhi kepercayaan individu terhadap lingkungan digital secara umum. Sejumlah penelitian menunjukkan bahwa korban kejahatan siber cenderung mengalami penurunan kepercayaan terhadap platform digital setelahnya, meningkatnya kewaspadaan berlebihan, hingga kecenderungan untuk menarik diri dari interaksi sosial daring maupun luring (Cazanis et al., 2025; Norris et al., 2019; Shang et al., 2022). Selain itu, pengalaman tersebut juga dapat memunculkan *distrust* atau perasaan skeptis terhadap nama institusi yang telah disalahgunakan untuk menipunya tersebut (Button et al., 2014; Lestari et al., 2024). Studi lain juga menunjukkan bahwa dampak psikologis seperti kecemasan, stres, dan isolasi sosial dapat berlangsung dalam jangka panjang setelah individu mengalami penipuan tersebut (Balakrishnan et al., 2025; Balcombe, 2025).

Hingga saat ini, penipuan berbasis *verified account* berbayar masih relatif jarang dikaji secara mendalam dan masih terbatas. Penelitian sebelumnya umumnya berfokus pada simbol digital yang memengaruhi kredibilitas di media sosial. Misalnya, model yang dikembangkan oleh Sundar (2008) menjelaskan bahwa simbol pada platform digital (seperti centang biru di sini) berfungsi sebagai isyarat sederhana yang digunakan pengguna untuk menilai kredibilitas secara instan. Penelitian lain juga mendukung bahwa pengguna cenderung mengandalkan isyarat sederhana dalam menilai kredibilitas di dunia maya, termasuk indikator dan legitimasi akun (Javed et al., 2024; Liu & Zheng, 2024). Temuan-temuan ini menunjukkan bahwa simbol verifikasi berperan sebagai penanda keaslian yang memengaruhi penilaian pengguna secara cepat. Namun demikian, studi-studi tersebut masih berfokus pada persepsi umum terhadap kredibilitas dan belum secara spesifik mengkaji bagaimana pengalihan fitur *verified account* berbayar dapat memengaruhi pengalaman psikologis korban dalam konteks penipuan daring seperti *spoofing* ini. Dengan demikian, masih terdapat kesenjangan dalam memahami bagaimana simbol verifikasi yang awalnya diasosiasikan dengan kepercayaan justru dapat dimanfaatkan dalam praktik penipuan.

Oleh karena itu, penelitian ini bertujuan untuk memahami bagaimana fitur *verified account* berbayar memengaruhi pembentukan persepsi positif korban terhadap pelaku kejahatan *spoofing* di media sosial X dan Telegram. Penelitian ini secara khusus menempatkan perspektif korban sebagai pusat analisis, dengan menggali bagaimana mereka memahami, memaknai, dan merespons keberadaan simbol verifikasi berbayar dalam pengalaman mereka. Fokus ini memungkinkan peneliti untuk melihat bagaimana perspektif korban, baik yang dipengaruhi oleh aspek kognitif, sosial, maupun emosional. Secara praktis, hasil riset ini diharapkan dapat meningkatkan literasi psikologis pengguna media sosial mengenai bagaimana fitur *verified account* berbayar dapat memengaruhi persepsi kepercayaan yang tidak kritis. Temuan ini juga diharapkan dapat memberikan masukan bagi platform terkait untuk merancang intervensi pencegahan kejahatan siber kepada para penggunanya.

METODE PENELITIAN

Variabel atau Konsep yang diteliti

Penelitian ini berfokus pada pengkajian konsep psikologis yang muncul dari pengalaman subjektif korban *spoofing*. Konsep utama yang diteliti adalah *trust bias*, yaitu kecenderungan individu untuk mempercayai pihak lain berdasarkan simbol digital, khususnya tanda *verified account* berbayar di media sosial. *Trust bias* dalam penelitian ini dipahami sebagai proses psikologis yang memengaruhi pembentukan kepercayaan korban terhadap pelaku *spoofing*. Selain itu, penelitian ini juga mengeksplorasi pemaknaan partisipan terhadap simbol verifikasi digital serta dampak yang dialami setelah penipuan.

Metode Sampling

Partisipan penelitian dipilih dengan menggunakan teknik *purposive sampling*, yakni pemilihan subjek berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian (Lenaini, 2021). Adapun kriteria partisipan adalah sebagai berikut: (1) Aktif menggunakan media sosial X atau Telegram, dan (2) Pernah mengalami penipuan daring (*spoofing*) yang dilakukan oleh pelaku yang memanfaatkan fitur *verified account* berbayar. Jumlah partisipan ditentukan berdasarkan prinsip *data saturation*, yaitu kondisi ketika data yang diperoleh menunjukkan pengulangan makna dan tidak menghasilkan tema baru yang signifikan (Naeem et al., 2024).

Subjek Penelitian

Subjek penelitian terdiri atas empat partisipan, yang meliputi dua pengguna media sosial Telegram dan dua pengguna media sosial X. Usia partisipan berkisar antara 16 hingga 25 tahun, dengan variasi jenis kelamin dan latar belakang. Seluruh partisipan merupakan korban langsung dari praktik *spoofing* yang dilakukan oleh akun berstatus *verified account* berbayar. Penelitian ini menggunakan desain kualitatif fenomenologi interpretatif, di mana peneliti berperan sebagai instrumen utama dalam proses pengumpulan dan analisis data. Relasi antara peneliti dan partisipan bersifat non-hierarkis dan tidak memiliki hubungan personal maupun profesional sebelum penelitian dilakukan. Data demografis ringkas partisipan disajikan pada Tabel 1.

Tabel 1. Profil Partisipan Penelitian

No.	Inisial	Usia	Jenis Kelamin	Platform
1.	IR	± 22 tahun	Perempuan	Telegram
2.	SR	± 22 tahun	Perempuan	Telegram
3.	AU	± 22 tahun	Perempuan	X
4.	SP	± 22 tahun	Laki-laki	X

Instrumen Penelitian

Instrumen utama dalam penelitian ini adalah panduan wawancara semi-terstruktur, yang disusun untuk memungkinkan eksplorasi pengalaman partisipan secara mendalam namun tetap terarah pada fokus penelitian (Moleong, 2019). Panduan wawancara mencakup tema-tema utama, antara lain:

- (1) persepsi partisipan terhadap akun bercentang biru;
- (2) pengalaman partisipan saat mengalami penipuan;
- (3) faktor-faktor yang memengaruhi kepercayaan terhadap pelaku; dan
- (4) dampak psikologis yang dirasakan setelah peristiwa *spoofing*.

Seluruh wawancara direkam dengan izin partisipan dan ditranskripsikan secara verbatim untuk keperluan analisis data. Selain itu, peneliti juga menggunakan catatan di lapangan dan dokumentasi terbatas yang relevan sebagai data pendukung.

Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif fenomenologi interpretatif, dengan fokus pada pemahaman mendalam mengenai pengalaman subjektif korban *spoofing* yang dilakukan oleh akun berstatus *verified account* berbayar di media sosial X dan Telegram. Pendekatan fenomenologi dipilih karena sesuai dengan tujuan penelitian, yaitu menggali makna pengalaman psikologis individu sebagaimana dipersepsikan dan ditafsirkan oleh partisipan, serta bagaimana pengalaman tersebut dipahami kembali melalui proses interpretasi peneliti (Kahija, 2017).

Pendekatan ini memungkinkan peneliti untuk memahami fenomena *trust bias* dan proses pembentukan kepercayaan korban terhadap simbol otoritas digital secara mendalam, tidak hanya sebagai peristiwa kejahatan siber, tetapi sebagai pengalaman psikologis yang bermakna bagi individu. Hal ini sejalan dengan pandangan (Smith et al., 2022) yang menyatakan bahwa fenomenologi interpretatif efektif digunakan untuk menelaah dinamika makna pengalaman subjektif dalam konteks sosial yang kompleks, termasuk interaksi di ruang digital.

Prosedur Pengambilan Data

Prosedur pengambilan data diawali dengan tahap persiapan penelitian, yang meliputi penyusunan panduan wawancara semi-terstruktur serta penjelasan tujuan dan ruang lingkup penelitian kepada calon partisipan. Sebelum pengambilan data dilakukan, peneliti meminta persetujuan partisipan (*informed consent*) sebagai bentuk pemenuhan prinsip etika penelitian, yang mencakup kesediaan partisipan untuk berpartisipasi secara sukarela, kerahasiaan data, serta hak partisipan untuk menghentikan keterlibatan dalam penelitian kapan pun tanpa konsekuensi.

Pengumpulan data dilakukan melalui wawancara semi-terstruktur yang memungkinkan eksplorasi pengalaman partisipan secara mendalam namun tetap terarah pada fokus penelitian. Wawancara dilaksanakan secara *hybrid*, yaitu secara daring dan luring, sesuai dengan kesepakatan bersama partisipan. Setiap partisipan mengikuti satu sesi wawancara dengan durasi minimal 45 menit dan maksimal 90 menit, dengan rata-rata durasi wawancara sekitar 60 menit. Seluruh proses wawancara direkam dengan izin partisipan dan kemudian ditranskripsikan secara verbatim untuk keperluan analisis data. Selama wawancara berlangsung, peneliti juga membuat catatan untuk menangkap konteks non-verbal dan refleksi awal terhadap data yang diperoleh.

Isu-isu etika penelitian dijaga dengan menerapkan prinsip anonimitas dan kerahasiaan data, di mana identitas partisipan disamarkan menggunakan inisial. Data yang diperoleh hanya digunakan untuk kepentingan akademik. Penelitian ini tidak melibatkan intervensi psikologis maupun kelompok rentan secara klinis, sehingga tidak memerlukan uji etik formal dari komite etik, namun tetap menjunjung tinggi standar etika penelitian psikologi.

Teknik Analisis Data

Analisis data dilakukan menggunakan *Interpretative Phenomenological Analysis (IPA)*, yang berfokus pada pemahaman mendalam mengenai bagaimana individu memaknai pengalaman hidupnya. IPA digunakan karena sejalan dengan kerangka fenomenologi interpretatif yang menekankan proses *double hermeneutic*, yakni partisipan berupaya memaknai pengalamannya, sementara peneliti menafsirkan makna tersebut secara reflektif (Smith et al., 2022).

Proses analisis dilakukan melalui enam tahapan, yaitu: (1) membaca dan membaca ulang (*reading and re-reading*), (2) pencatatan awal (*initial noting*), (3) pengembangan tema-tema emergen (*developing emergent themes*), (4) pencarian hubungan antar tema (*searching for connections*), (5) analisis kasus berikutnya (*moving to the next cases*), dan (6) pencarian pola lintas kasus (*looking*

for patterns across cases). Peneliti berperan sebagai instrumen utama dalam proses interpretasi, dengan tetap menjaga reflektivitas selama analisis berlangsung.

Keabsahan data dijaga melalui dua teknik utama, yaitu *member checking*, dengan mengonfirmasi ringkasan hasil wawancara kepada partisipan untuk memastikan kesesuaian makna, serta triangulasi data, dengan membandingkan hasil wawancara, observasi ringan, dan dokumentasi berupa bukti percakapan yang relevan (Sidiq & Choiri, 2019). Langkah-langkah ini dilakukan untuk meningkatkan kredibilitas dan keandalan temuan penelitian, sehingga hasil yang diperoleh benar-benar merepresentasikan pengalaman psikologis partisipan.

HASIL PENELITIAN

Tema 1: Merasa Aman dengan Simbol Digital

Hasil analisis menunjukkan bahwa kepercayaan korban terhadap pelaku *spoofing* dibangun melalui pemaknaan simbolik terhadap tanda centang biru sebagai representasi status, legitimasi, dan keamanan di ruang digital. Bagi para korban, keberadaan *verified account* berbayar tidak hanya dipahami sekadar sebagai fitur platform saja, melainkan sebagai penanda sosial yang diasosiasikan dengan status ekonomi, profesionalitas, dan moralitas pelaku. Pemaknaan ini menciptakan rasa aman awal yang membuat korban menurunkan kewaspadaan dalam proses interaksi dan pengambilan keputusan.

Korban IR memaknai akun bercentang biru sebagai indikator kemampuan finansial pelaku. Kesiapan pelaku untuk membayar layanan *verified account* ditafsirkan sebagai bukti bahwa pelaku memiliki sumber ekonomi yang memadai, sehingga dianggap kecil kemungkinan untuk melakukan penipuan. Dalam pengalaman IR, kemampuan finansial pelaku dimaknai sebagai karakter moral yang positif, di mana “orang yang mampu” dipersepsikan tidak memiliki kebutuhan untuk melakukan tindakan curang.

“Bisa dibilang karena di akun yang bercentang biru yang saya percayanya dia orang yang punya budget...” (IR)

“...Kalau yang centang biru tuh lebih meyakinkan gitu. Lebih kayak dia punya uang dan kelihatan punya bisnis gitu...” (IR)

Pemaknaan serupa juga diperkuat oleh indikator simbolik lain yang dimiliki pelaku, seperti kepemilikan *username fragment* di Telegram yang bernilai tinggi. Bagi IR, kepemilikan aset digital tersebut semakin menegaskan citra pelaku sebagai individu yang berkecukupan dan berstatus sosial tinggi, sehingga secara psikologis semakin menjauhkan pelaku dari stereotip sebagai penipu.

“...Jadi itulah, karena itu saya anggap dia kaya karena dia punya banyak username fragment dan pengguna telegram premium.” (IR)

“...kaya enggak sayang gitu dia pakai uangnya. Kalau dia mau itu ya dia beli ya...” (IR)

Pandangan IR sejalan dengan pengalaman SR, yang juga memaknai akun bercentang biru sebagai representasi kemapanan ekonomi. Dalam kerangka berpikir SR, kemapanan ekonomi diasosiasikan dengan rendahnya motif untuk melakukan penipuan, sehingga status “orang kaya” berfungsi sebagai justifikasi kognitif untuk mempercayai pelaku.

“Biasanya orang-orang menganggap kaya.” (SR)

“Kalau dalam istilah kasarnya orang kaya tidak terlalu butuh duit lagi, jadi tidak mungkin nipu, ngapain nipu.” (SR)

Selain dimaknai sebagai simbol kemapanan, *verified account* juga dipersepsikan sebagai penanda keaktifan dan keberlangsungan akun. Korban IR dan SR memandang akun bercentang biru sebagai akun yang “serius” dan tidak mudah menghilang, berbeda dengan akun tanpa verifikasi yang diasosiasikan dengan akun bodong atau akun sementara yang digunakan untuk menipu lalu dihapus. Persepsi ini memperkuat rasa aman korban karena pelaku dianggap memiliki identitas digital yang stabil dan dapat ditelusuri.

“Kalau nggak centang biru, sekarang tuh kayak keangap akun bodong gitu. Atau malah second akun second yang itu kayak rawan banget kan. Akun second itu buat nipu sekali terus langsung di-deact-in gitu.” (IR)

“Kalau di dunia telegram sendiri, kasus-kasus penipuan itu banyak dilakukan akun bodong. Misalnya username-nya asal-asalan, setup-nya asal-asalan. Tujuannya mereka biar bisa untuk secara cepat mengganti. Mengganti username-nya atau bahkan menghapus akunnya. Jadi kalau memang akun premium kan agak sulit untuk melakukan hal-hal yang seperti yang dilakukan oleh akun-akun bodong, akun-akun biasa.” (SR)

Pemaknaan simbol otoritas digital juga muncul pada korban SP dan AU di platform X. SP mengungkapkan bahwa akun terverifikasi dipersepsikan sebagai akun yang telah terdaftar secara resmi oleh platform, sehingga dianggap aman dan tidak termasuk kategori akun penipuan. Status verifikasi tersebut juga diasosiasikan dengan popularitas dan reputasi, di mana akun bercentang biru dipandang sebagai “akun besar” yang memiliki privilese dan nama baik yang harus dijaga.

“Orang dengan verified adalah orang yang istilahnya terpercaya gitu lah, bukan akun scam gitu.” (SP)

“...kalau ada verified itu kan berarti orangnya orang yang penting lah atau orang yang punya privilege gitu kan...” (SP)

“Karena kebanyakan akun centang biru di ranah penjualan ini, mempunyai banyak followers dan following yang terkenal. Ibaratnya akun tsb adalah “akun besar”.” (AU)

Secara keseluruhan, tema ini menunjukkan bahwa kepercayaan korban tidak dibangun melalui proses verifikasi rasional terhadap identitas pelaku, melainkan melalui pemaknaan simbolik terhadap tanda-tanda visual dan status digital. Simbol otoritas digital seperti centang biru, kepemilikan aset digital, dan popularitas akun berfungsi sebagai *heuristic cue* yang memfasilitasi terbentuknya rasa aman semu. Dalam konteks ini, *verified account* berbayar menjadi sumber bias kepercayaan yang secara tidak disadari memengaruhi penilaian korban terhadap kredibilitas pelaku.

Tema 2: Profesionalitas Semu sebagai Dasar Kepercayaan

Analisis menunjukkan bahwa kepercayaan korban terhadap pelaku tidak hanya dibangun melalui simbol otoritas digital, tetapi juga melalui pengalaman interaksi yang terasa profesional, meyakinkan, dan akrab secara emosional. Bagi korban, cara pelaku menawarkan harga, menampilkan bukti transaksi, serta membangun pola komunikasi yang responsif dan ramah dimaknai sebagai tanda itikad baik dan kredibilitas. Pengalaman ini menciptakan kesan bahwa interaksi yang berlangsung merupakan transaksi yang wajar dan aman, sehingga mengurangi kecenderungan korban untuk bersikap kritis.

Dalam pengalaman IR sebagai penjual, tawaran harga tinggi dari pelaku menjadi sinyal psikologis yang memperkuat persepsi bahwa pelaku adalah individu berkecukupan dan serius dalam bertransaksi. Harga tinggi tidak sekadar dipahami sebagai nilai ekonomi, melainkan sebagai penanda komitmen yang menegaskan keaslian niat pelaku.

“...Nah, karena dia menawarkan harga yang tinggi, jadi saya tergiur lah itu sama harga yang ditawarkan...” (IR)

“...Awalnya saya kan kayak nggak dijual sebelum ditawarin harga tinggi gitu kan...” (IR)

Sebaliknya, bagi korban yang berperan sebagai pembeli, daya tarik utama justru terletak pada penawaran harga yang lebih rendah dari harga pasar atau adanya potongan harga. Harga yang dianggap masuk akal dan menguntungkan ini dimaknai sebagai kesempatan yang sayang untuk dilewatkan, sehingga membangun rasa percaya dan urgensi untuk segera bertransaksi.

“Pertama karena memang akun tersebut menawarkan harga yang lebih miring...” (SP)

“...Saya menemukan seller yang akun centang biru dan daftar pricelist nya yang lumayan affordable untuk harga pasaran biasa...” (AU)

“Potongan harga pastinya. Potongan harga. Harga promo.” (SR)

Kepercayaan korban semakin diperkuat oleh keberadaan testimoni palsu yang ditampilkan oleh pelaku. Banyaknya testimoni dipersepsikan sebagai bukti sosial bahwa pelaku telah dipercaya oleh orang lain sebelumnya. Dalam pengalaman korban, testimoni tersebut berfungsi sebagai jaminan psikologis yang menenangkan keraguan, meskipun keaslian testimoni tidak diverifikasi secara mendalam.

“...Nah, saya buka dan ya proofnya banyak gitu. Proofnya banyak, dan si akunnya pihak ketiga itu kayak meyakinkan gitu kan...” (IR)

“Mungkin kalau saya tidak salah, sekitar 60 atau 80 testimoni yang dibuat di channel private.” (SR)

“...Jadi saya cek akunnya, akunnya verified, kemudian saya cek juga dari testimoninya juga udah banyak yang berlangganan ke akun tersebut...” (SP)

“...terakhir saya cek testimoni beliau lumayan banyak. Jadi itu yang bikin saya yakin, Kak.” (AU)

Setelah mengalami penipuan, sebagian korban baru menyadari bahwa testimoni yang mereka anggap meyakinkan tersebut dapat diperdagangkan dan dimanipulasi. Kesadaran ini muncul sebagai refleksi retrospeksi, di mana korban menilai kembali bahwa rasa aman yang mereka rasakan sebelumnya dibangun di atas bukti sosial yang semu.

“Setelah saya tertipu, saya baru search dari orang-orang kalau ternyata ada oknum-oknum yang memperjualbelikan testimoni.” (SR)

“Iya. Jadi ada beberapa seller yang tidak mau berjualan lagi. Nah, testimoninya itu mereka jual dan itu yang dipakai oleh penipu.” (SR)

Selain faktor harga dan testimoni, pola komunikasi pelaku memainkan peran penting dalam membangun keakraban emosional. Korban memaknai gaya komunikasi pelaku yang santai, ramah, serta penggunaan bahasa yang selaras dengan gaya korban sebagai tanda kedekatan dan kejujuran. Teknik *mirror communication* ini menciptakan kesan bahwa pelaku satu frekuensi dengan korban, sehingga interaksi terasa alami dan tidak mencurigakan.

“...dia juga menggunakan bahasa-bahasa yang membuat kita nyaman. Jadi dia tidak terlalu kaku. Dia kayak mirror typing mengikuti alur, jadi kita juga merasa asik untuk berkomunikasi dengan dia.” (SR)

“Ya, sama kayak orang mau beli...” (IR)

“Iya, pada saat itu memang dia memberikan bahasa-bahasa yang umumnya memang digunakan oleh anak-anak muda zaman sekarang sih. Pake emot- emot atau pake tanda-tanda yang menunjukkan kalau dia adalah seorang yang ramah...” (SP)

“Betul kak, bahasa yang digunakan dan waktu balas yang sangat cepat membuat saya percaya...” (AU)

Respons yang cepat dan konsisten dari pelaku semakin memperkuat citra profesional dan dapat diandalkan. Bagi korban, kecepatan respons dimaknai sebagai bentuk keseriusan dan komitmen dalam bertransaksi, sehingga semakin menguatkan rasa percaya terhadap pelaku.

“Itu awalnya sellernya juga baik kok Mbak, beneran deh. Sellernya itu enak, ramah, baik gitu kan...” (IR)

“Selain fast respon, dia juga menggunakan bahasa-bahasa yang membuat kita nyaman...” (SR)

“Pada saat sebelum kejadian penipuan memang yang dilakukan sellernya itu cukup fast response...” (SP)

“Saya tertarik dan menghubungi beliau lewat DM, seperti biasa awal-awal beliau sangat fastrespon dan ramah.” (AU)

Secara keseluruhan, tema ini menunjukkan bahwa kepercayaan korban dibangun melalui pengalaman interaksi yang tampak profesional dan akrab, meskipun pada akhirnya bersifat semu. Harga yang menarik, testimoni yang meyakinkan, serta komunikasi yang ramah dan responsif berfungsi sebagai *heuristic cues* yang memperkuat rasa aman psikologis korban. Dalam konteks ini, pelaku tidak hanya memanfaatkan fitur teknis platform, tetapi juga memanipulasi dinamika interaksi sosial untuk membentuk kepercayaan korban secara emosional.

Tema 3: Ilusi dalam Pengambilan Keputusan

Hasil analisis menunjukkan bahwa pengalaman korban terhadap kejahatan *spoofing* juga dipengaruhi oleh kondisi internal yang membentuk rasa aman subjektif dan ilusi kontrol dalam pengambilan keputusan. Pada saat kejadian berlangsung, seluruh partisipan mengungkapkan bahwa mereka berada dalam kondisi ekonomi yang relatif stabil atau “mampu”. Kondisi ini dimaknai sebagai kemampuan personal untuk menanggung risiko, sehingga secara tidak langsung menurunkan tingkat kewaspadaan terhadap potensi kerugian.

“Lagi mampu.” (IR)

“Kalau di saat itu mampu.” (SR)

“...menurut saya pada saat itu kondisi ekonomi saya sedang lebih baik dari yang sekarang gitu.” (SP)

“Alhamdulillah saat itu memang lg lancar keuangan nyaa.” (AU)

Bagi sebagian korban, rasa mampu secara finansial menciptakan keyakinan bahwa kerugian yang mungkin terjadi masih berada dalam batas yang dapat ditoleransi. Uang yang digunakan dipersepsikan sebagai uang pribadi atau tabungan, sehingga kehilangan tersebut dianggap tidak akan berdampak signifikan terhadap kondisi hidup secara keseluruhan. Pemaknaan ini membentuk ilusi kontrol, di mana korban merasa tetap memiliki kendali meskipun menghadapi risiko penipuan.

“Ya, pastinya gitu sih. Kalau misal selain itu juga, itu kan uang saya pribadi gitu kan, uang saya tabungan pribadi, dan gak ada siapapun yang tahu gitu. Jadi kalau hilang atau gimana ya yaudah gitu...” (IR)

“Mungkin bisa jadi iya juga, karena pada saat itu juga saya mikir oke lah kalau segini mungkin masih bisa disisiin lagi buat bulan depan gitu, buat beli lagi gitu...” (SP)

Selain rasa mampu secara finansial, sebagian korban juga membangun rasa aman melalui keberadaan pihak ketiga atau rekening bersama (*rekber*) dalam proses transaksi. Penggunaan *rekber* dimaknai sebagai mekanisme perlindungan tambahan yang diyakini dapat meminimalkan risiko penipuan. Kehadiran pihak ketiga ini memberi korban keyakinan bahwa transaksi berada dalam pengawasan dan kontrol pihak lain yang dianggap netral..

“...saya akan menggunakan pihak ketiga yaitu admin Rekber...” (SR)

“...Ngiranya udah ada saksi ketiga jadinya aman gitu kan...” (IR)

Dalam pemahaman korban, sistem *rekber* berfungsi sebagai penjamin keamanan dana hingga transaksi selesai. Namun, pengalaman penipuan menunjukkan bahwa asumsi keamanan tersebut tidak selalu sesuai dengan realitas, terutama ketika pihak ketiga justru terlibat dalam praktik manipulatif bersama pelaku.

“Ternyata mereka yang pihak ketiga sama si pembeli itu sekongkol...” (IR)

“...dan yang pihak ketiga harusnya transfer bayarannya ke saya gitu kan, tapi ternyata tidak...” (IR)

Selain itu, korban juga memaknai upaya pelaku untuk menampilkan akun bercentang biru sebagai bentuk investasi yang tidak mungkin dilakukan untuk tujuan menipu. Tampilan visual akun yang dianggap “bagus” dan “premium” memperkuat keyakinan korban bahwa pelaku memiliki niat yang *legitimate*. Pemaknaan ini menunjukkan bagaimana daya tarik visual dan simbol status digital membentuk bias persepsi terhadap risiko.

“...mereka nggak mungkin nipu karena mereka aja akunnya premium. Maksudnya mereka beli akun bagus-bagus agar untuk dipercaya, bukan menipu.” (SR)

“...karena kan kalau di Twitter tuh pakai verified itu kalau gak salah kan bayar juga ya ke Twitternya gitu. Jadi itu ya saya percaya kalau dia udah rela bayar buat akunnya itu terpercaya berarti...” (SP)

“Menurut pandangan saya, mereka yang berlangganan centang biru mungkin pertama kali tergiur karena icon centang biru yang terlihat “bagus” untuk di akun mereka...” (AU)

Karakteristik personal korban turut memengaruhi proses pengambilan keputusan. Beberapa korban mengakui adanya kecenderungan impulsif dan pengalaman sebelumnya pernah tertipu, yang memengaruhi cara mereka merespons situasi transaksi daring. Dalam konteks ini, pengalaman masa lalu tidak selalu meningkatkan kewaspadaan, tetapi justru dapat menormalisasi risiko penipuan sebagai bagian dari pengalaman bertransaksi di dunia digital.

“...Karena menurut saya juga mama saya itu impulsif pun juga saya demikian...” (SP)

“Sebenarnya saya sering ditipu, Kak.” (AU)

Secara keseluruhan, tema ini menggambarkan bahwa kepercayaan korban tidak hanya dipengaruhi oleh faktor eksternal dan simbol otoritas digital, tetapi juga oleh rasa mampu, keyakinan akan kontrol, serta karakteristik personal yang membentuk cara korban memaknai risiko. Ilusi kontrol yang muncul dari kondisi finansial, penggunaan pihak ketiga, dan kepercayaan terhadap simbol visual memperkuat kerentanan psikologis korban terhadap kejahatan *spoofing*. Temuan ini menegaskan bahwa *spoofing* merupakan fenomena psikologis yang kompleks, di mana bias kognitif dan emosional berperan penting dalam pembentukan keputusan dan kepercayaan di media sosial.

PEMBAHASAN

Perkembangan interaksi di dunia maya telah mengubah cara individu membangun dan menilai kepercayaan mereka di jagat media sosial, terutama dengan hadirnya berbagai fitur yang merepresentasikan identitas dan kredibilitas pengguna, seperti fitur *verified account* berbayar. Hadirnya berbagai perkembangan kebaruan tersebut, tidak luput menghadirkan juga celah kejahatan yang baru. Salah satunya adalah kejahatan *spoofing*, yaitu tindakan penyamaran identitas untuk memperoleh kepercayaan korban. Dalam konteks penelitian ini, *spoofing* dimaknai ketika pelaku membangun citra sebagai akunerverifikasi untuk menciptakan kesan kredibel. Kepercayaan yang terbentuk tersebut kemudian dimanfaatkan pelaku untuk melakukan penipuan, sebagaimana dialami oleh para korban dalam penelitian ini. Oleh karena itu, pembahasan ini tidak berfokus pada sebab-akibat semata, melainkan pada bagaimana korban memaknai simbol, interaksi, dan kondisi internal yang membentuk persepsi kepercayaan mereka.

Hasil penelitian menunjukkan bahwa tanda centang biru dimaknai oleh seluruh partisipan sebagai simbol keaslian, kredibilitas, dan status sosial tertentu. Dalam pengalaman korban, simbol ini secara psikologis memicu *trust bias*, yaitu kecenderungan mempercayai pihak lain berdasarkan sesuatu yang mereka asosiasikan dengan legitimasi. Para korban tersebut secara otomatis mengenali tanda centang biru sebagai hal yang dapat dipercaya. Fenomena ini memperlihatkan bahwa kepercayaan di dunia digital tidak selalu hanya dapat dibangun melalui interaksi yang intens dan mendalam saja, melainkan juga melalui representasi status dari tampilan luarnya. Misalnya, korban IR dan SR memaknai akun bercentang biru sebagai representasi individu yang berkecukupan secara ekonomi, dan karena itu, mereka dianggap ‘tidak mungkin menipu’. Pemaknaan ini juga menunjukkan adanya *heuristic trust bias*, yakni kecenderungan untuk menarik kesimpulan atau keputusan secara tidak sadar dari petunjuk sederhana yang mereka percayai, alih-alih dari evaluasi yang objektif dan mendalam (Gigerenzer & Gaissmaier, 2011; Kahneman, 2011).

Dalam konteks ini, centang biru berfungsi sebagai *cue of authenticity* yang secara otomatis memicu *automatic trust response* (Hoq et al., 2025; Metzger & Flanagin, 2013; Sundar, 2008). Dalam perspektif psikologi kognitif, *cue of authenticity* bekerja sebagai pemicu awal yang mengarahkan individu untuk melakukan penilaian cepat terhadap suatu objek atau sumber informasi. Ketika individu menemukan simbol yang diasosiasikan dengan legitimasi, seperti centang biru tersebut, proses kognitif cenderung disederhanakan melalui penggunaan heuristik (Gigerenzer & Gaissmaier, 2011; Traberg et al., 2024). Hal ini kemudian memunculkan *automatic trust response*, yaitu kecenderungan untuk langsung mempercayai tanpa melalui proses verifikasi yang kritis dan mendalam (Kahneman, 2011). Mekanisme ini menunjukkan bahwa dalam konteks digital, kepercayaan dapat terbentuk secara instan dan tidak selalu melalui pertimbangan rasional, sehingga membuka peluang terjadinya kesalahan penilaian terhadap kredibilitas suatu akun.

Selain itu, sebagian besar korban juga memersepsikan akun bercentang biru sebagai ‘akun besar’ yang memiliki banyak pengikut dan reputasi tinggi. Persepsi ini selaras dengan teori *parasocial trust*, di mana pengguna cenderung mempercayai akun yang tampak berpengaruh karena diasosiasikan dengan otoritas sosial (Hoffner & Bond, 2022). Dalam konteks ini, *trust bias* beroperasi serupa dengan *halo effect*, yaitu kecenderungan di mana satu atribut positif dapat memengaruhi penilaian positif lainnya (Thorndike, 1920), seperti kredibilitas atau kejujuran, sehingga sesuatu yang ‘terlihat baik’ diasumsikan ‘dapat dipercaya’. Proses ini dapat dipahami melalui kerangka *dual-process theory* yang menjelaskan bahwa manusia memiliki dua cara dalam mengambil keputusan, yaitu pemrosesan cepat, intuitif, dan otomatis (disebut dengan System 1), serta pemrosesan yang lebih lambat, analitis, dan reflektif (disebut dengan System 2) (Kahneman, 2011). Dengan demikian, para korban cenderung tidak mengamati, mengevaluasi atau melakukan *cross-check* dalam berinteraksi (System 2), melainkan mereka cenderung langsung mengadili berdasarkan intuisi dan penilaian emosional singkat mereka saja (System 1). Dalam konteks temuan ini, kepercayaan yang muncul pada korban lebih banyak didorong oleh pemrosesan intuitif tersebut, dibandingkan evaluasi rasional yang mendalam. Akibatnya, korban menunjukkan bentuk *illusory trust*, yaitu kepercayaan semu yang muncul karena rasa familier terhadap centang biru yang dikaitkan dengan prestise dan keaslian.

Lebih lanjut, temuan penelitian menunjukkan bahwa kepercayaan korban tidak hanya dibentuk oleh persepsi individual saja, tetapi juga diperkuat melalui strategi komunikasi dan manipulasi situasional yang dilakukan oleh pelaku. Partisipan memaknai tawaran harga yang jauh dari pasaran sebagai peluang yang menguntungkan. Pemaknaan ini selaras dengan prinsip *reciprocity bias* dan *scarcity effect* dalam teori persuasi, di mana individu cenderung merespons positif terhadap keuntungan instan atau kesempatan yang dianggap langka (Cialdini, 2021). *Reciprocity bias* merujuk pada kecenderungan individu untuk membalas perlakuan atau keuntungan yang diterima, sehingga tawaran yang tampak ‘menguntungkan’ dipersepsikan sebagai niat baik yang perlu direspons secara positif. Sementara itu, *scarcity effect* menunjukkan bahwa sesuatu yang dipersepsikan terbatas atau langka akan dinilai lebih bernilai dan lebih mendesak untuk segera diambil keputusan. Kombinasi kedua mekanisme ini menyebabkan korban tidak hanya merasa terdorong untuk merespons secara sosial, tetapi juga merasa perlu bertindak lebih cepat, sehingga mengurangi kesempatan untuk melakukan evaluasi yang lebih kritis. Akibatnya, keputusan untuk melanjutkan interaksi atau transaksi menjadi lebih impulsif dan rentan terhadap manipulasi.

Selain itu, keberadaan testimoni palsu dimaknai sebagai bukti sosial bahwa akun tersebut dapat dipercaya. Hal ini mencerminkan mekanisme *social proof*, di mana individu menilai keabsahan suatu tindakan berdasarkan persepsi bahwa orang lain telah melakukannya terlebih dahulu dan aman (Cialdini, 2021; Liu, 2025). Dalam ruang digital, *social proof* ini dapat dibentuk secara artifisial, dicolong, atau bahkan diperjualbelikan, sehingga meskipun tidak didasarkan pada realitas yang sebenarnya namun tetap

memperkuat persepsi legitimasi dari para korban. Secara psikologis, *social proof* bekerja dengan mengurangi ketidakpastian, terutama dalam situasi ambigu, sehingga individu cenderung menggunakan perilaku orang lain sebagai acuan dalam mengambil keputusan. Ketika korban melihat adanya testimoni, hal tersebut diinterpretasikan sebagai indikator bahwa akun tersebut telah dipercaya oleh banyak orang. Kondisi ini menciptakan ilusi konsensus sosial, di mana sesuatu dianggap benar atau aman karena terlihat ‘banyak yang melakukan’, meskipun informasi tersebut sebenarnya dimanipulasi. Akibatnya, korban menjadi lebih mudah mengabaikan keraguan awal dan terdorong untuk mengikuti keputusan yang tampak telah divalidasi secara sosial.

Aspek komunikasi juga menjadi bagian penting dalam pengalaman kepercayaan korban. Pelaku mempraktikkan *mirror communication* dengan menyesuaikan gaya bahasa, penggunaan emotikon, serta kecepatan respons agar menyerupai pola komunikasi korban. Strategi ini tidak hanya menciptakan kesan kesamaan (*perceived similarity*), tetapi juga meningkatkan rasa kehangatan yang secara signifikan berkontribusi pada pembentukan kepercayaan dalam interaksi digital (Ahmad, 2026; Valori et al., 2024). Penelitian terbaru menunjukkan bahwa kesamaan gaya komunikasi dan timbal balik dalam interaksi (*reciprocal communication*) dapat meningkatkan *interpersonal liking* (ketertarikan antarpribadi) dan secara langsung memperkuat kepercayaan, bahkan dalam interaksi singkat dengan orang asing di media sosial. Kondisi ini kemudian memicu terbentuknya *affective trust*, yaitu kepercayaan yang didasarkan pada kedekatan emosional, rasa nyaman, dan persepsi adanya niat baik dari pihak lain (McAllister, 1995). Lebih jauh, keselarasan komunikasi tersebut secara tidak langsung menurunkan kewaspadaan korban, karena interaksi yang terasa familier cenderung diasosiasikan sebagai rasa aman dan dapat dipercaya. Dalam konteks ini, korban juga mengevaluasi kredibilitas berdasarkan pengalaman emosional selama berinteraksi. Hal ini menunjukkan bahwa kejahatan *spoofing* tidak semata-mata bersifat teknis, melainkan melibatkan *psychological engineering*, yaitu manipulasi sistematis terhadap emosi, persepsi sosial, dan dinamika interaksi untuk membangun kredibilitas semu (Hancock, 2012).

Selain pengalaman eksternal yang dialami korban, penelitian ini juga mengungkap bagaimana partisipan memaknai kondisi internal diri mereka pada saat peristiwa *spoofing* itu terjadi. Kondisi internal tersebut tidak diposisikan sebagai penyebab tunggal, melainkan sebagai bagian dari konteks subjektif yang membentuk pengalaman korban. Dalam refleksi partisipan, kondisi ekonomi yang relatif stabil dimaknai sebagai rasa aman personal, yang membuat mereka tidak terlalu mengantisipasi kemungkinan terjadinya penipuan. Temuan ini terlihat pada beberapa partisipan yang secara eksplisit menyatakan bahwa mereka merasa “tidak mungkin menjadi target” atau “mampu menanggung kerugian” sehingga tidak merasa perlu melakukan verifikasi lebih lanjut dalam berinteraksi dengan akun tersebut. Secara psikologis, pengalaman ini menunjukkan munculnya *false sense of security*, yaitu perasaan aman yang berlebihan sehingga menurunkan tingkat kewaspadaan individu terhadap risiko. Fenomena ini sejalan dengan konsep *optimism bias*, di mana individu cenderung meyakini bahwa dirinya lebih kecil kemungkinannya mengalami peristiwa negatif dibandingkan orang lain (Sharot, 2011). Studi lain menunjukkan bahwa rasa percaya diri berlebih terhadap kemampuan pribadi dalam mengelola risiko dapat membuat individu mengabaikan potensi ancaman yang sebenarnya (Arachchilage & Love, 2014). Dalam konteks penelitian ini, persepsi keamanan diri yang dimiliki partisipan justru berkontribusi pada berkurangnya evaluasi kritis terhadap situasi yang dihadapi, sehingga memperkuat kecenderungan untuk mempercayai pelaku kriminal.

Selain itu, beberapa partisipan memaknai penggunaan jasa pihak ketiga (rekening bersama) sebagai bentuk perlindungan tambahan dalam transaksi daring. Kepercayaan terhadap pihak ketiga ini dipandang sebagai cara untuk menciptakan rasa aman, meskipun pada akhirnya justru menjadi sumber kerentanan masalah ketika pihak tersebut merupakan pihak fiktif yang bersekongkol. Fenomena ini dapat dipahami sebagai bentuk *delegation of trust*, yaitu ketika individu menyerahkan tanggung jawab keamanan kepada pihak lain sehingga kontrol terhadap risiko menjadi berkurang (Hoff & Bashir, 2015). Di sisi lain, beberapa partisipan juga merefleksikan bahwa mereka cenderung impulsif dan mudah percaya. Refleksi ini tidak hanya menunjukkan kelemahan personal, tetapi juga menggambarkan pola pengambilan keputusan yang dipengaruhi oleh pemikiran dangkal semata. Dalam konteks ini, pengalaman korban selaras dengan konsep *low cognitive reflection* (Frederick, 2005), yaitu kecenderungan mengambil keputusan secara cepat tanpa pertimbangan mendalam, terutama ketika dihadapkan pada simbol legitimasi seperti centang biru atau testimoni yang tampak meyakinkan.

Temuan ini mengindikasikan bahwa kepercayaan digital mencerminkan adanya *social trust necessity*, yaitu kebutuhan psikologis individu untuk merasa terhubung, aman, dan dapat mempercayai orang lain dalam interaksi sosial, yang pada saat yang sama juga membuka celah bagi terjadinya kejahatan siber. Dalam perspektif psikologi sosial, manusia secara alami memiliki kecenderungan untuk membangun kepercayaan sebagai mekanisme untuk mengurangi ketidakpastian dan mempermudah interaksi, termasuk dalam interaksi digital. Kebutuhan ini menjadi semakin menonjol di ruang digital yang minim interaksi secara langsung, sehingga individu cenderung mengandalkan simbol saja sebagai substitusi dari interaksi tatap muka. Akibatnya, dorongan untuk tetap mempercayai dalam kondisi terbatas atau ambigu menjadi semakin kuat. Dalam konteks ini, temuan penelitian juga memperkuat konsep *digital deception* yang dikemukakan oleh (Hancock, 2012), bahwa manipulasi modern tidak lagi semata-mata bersifat teknis, melainkan lebih banyak memanfaatkan strategi psikologis seperti pengelolaan kesan (*impression management*) dan pembentukan kepercayaan. Pelaku tidak lagi menipu melalui perangkat lunak, tetapi melalui rekayasa emosi dan persepsi pengguna. Lebih lanjut, hasil ini selaras dengan penelitian terbaru yang menunjukkan bahwa simbol verifikasi di media sosial dapat secara signifikan meningkatkan persepsi dan kepercayaan pengguna, bahkan tanpa adanya bukti validasi yang kuat (Geels et al., 2024; Liao et al., 2024).

Fitur *verified account* berbayar berfungsi sebagai *false trust symbol*, yaitu simbol digital yang berpotensi menipu mekanisme penilaian sosial pengguna. Dalam konteks psikologi siber, temuan ini mencerminkan adanya pergeseran *locus of trust*, yaitu pusat

atau sumber kepercayaan individu, dari yang semula berbasis pada interaksi tatap muka dan bukti langsung, menjadi bergeser ke atribut-atribut digital seperti tampilan akun dan simbol verifikasi (Metzger & Flanagin, 2013; Sundar, 2008). Akibatnya, korban *spoofing* tidak lagi menilai identitas pelaku berdasarkan bukti faktual, melainkan cukup dari tampilan yang diasosiasikan positif, seperti centang biru ini. Kondisi ini menunjukkan bahwa dalam lingkungan digital, individu cenderung mengandalkan *heuristic cues*, yaitu petunjuk sederhana atau isyarat cepat (misalnya simbol verifikasi, jumlah pengikut, atau tampilan akun) yang digunakan untuk menilai kredibilitas tanpa melalui proses evaluasi yang mendalam (Gigerenzer & Gaissmaier, 2011; Traberg et al., 2024). Lebih lanjut, pola ini mengindikasikan adanya *trust distortion* di ruang digital, yaitu kondisi di mana *status cues* (seperti simbol verifikasi atau popularitas) menggantikan *authentic cues* (seperti bukti identitas yang valid) dalam membentuk persepsi kredibilitas. Temuan ini sejalan dengan penelitian terbaru yang menunjukkan bahwa isyarat sosial dan visual di media digital dapat secara signifikan memengaruhi persepsi kepercayaan, bahkan ketika isyarat tersebut tidak mencerminkan realitas yang sebenarnya (Chu et al., 2025). Dengan demikian, permasalahan utama tidak hanya terletak pada keberadaan simbol itu sendiri, tetapi pada cara simbol tersebut diinterpretasikan secara heuristik oleh pengguna, sehingga membuka ruang bagi manipulasi dan eksploitasi dalam kejahatan *spoofing* tersebut.

Secara keseluruhan, pengalaman para korban *spoofing* tersebut memperlihatkan bagaimana mekanisme kepercayaan tradisional sebenarnya tidak hilang, melainkan juga beradaptasi dan berpindah ke ranah digital. Tanda centang biru tidak lagi sekadar ikon validasi, tetapi berfungsi sebagai status sosial yang memicu rasa aman dan keaslian. Namun, karena kebutuhan untuk percaya manusia bersifat mendasar, simbol ini menjadi sangat rentan untuk dimanfaatkan secara manipulatif oleh pelaku kejahatan. Terlebih lagi ketika akses terhadap fitur *verified account* tersebut dapat diperoleh secara bebas melalui skema berbayar. Kondisi ini menunjukkan bahwa celah utama berakar pada kecenderungan psikologis individu untuk tetap percaya meskipun berada dalam situasi yang tidak sepenuhnya pasti. Kehadiran fitur *verified account* berbayar tersebut pada akhirnya justru memperparah dan memperbesar celah dari modus kejahatan itu. Dengan demikian, hasil ini memiliki implikasi penting bagi kebijakan platform media sosial. Simbol verifikasi sebaiknya dibedakan antara yang asli dan berbayar, misalnya melalui perbedaan warna, label, atau keterangan tambahan. Pembedaan ini dapat membantu pengguna menilai kredibilitas akun secara lebih akurat dan menurunkan risiko kejahatan seperti *spoofing*.

KESIMPULAN

Fitur *verified account* berbayar telah menggeser makna simbol verifikasi dari penanda keaslian menjadi sekadar atribut digital yang dapat dimanipulasi, sehingga memicu *trust bias* dan ketergantungan pada *heuristic cues* (simbol sederhana) dalam menilai kredibilitas. Akibatnya, korban cenderung membangun kepercayaan semu tanpa verifikasi mendalam, yang diperkuat oleh strategi manipulasi pelaku seperti penggunaan testimoni palsu, harga menarik, dan komunikasi yang meyakinkan. Temuan ini menunjukkan bahwa kepercayaan di ruang digital tidak hanya dipengaruhi oleh simbol eksternal, tetapi juga oleh kebutuhan psikologis untuk percaya (*social trust necessity*). Dengan demikian, fitur *verified account* berbayar berpotensi menjadi *false trust symbol* yang memperbesar risiko kejahatan *spoofing*, sehingga diperlukan kebijakan platform yang mampu membedakan secara jelas antara verifikasi autentik dan berbayar guna meningkatkan akurasi penilaian kredibilitas pengguna.

Ucapan Terima Kasih

Peneliti mengucapkan terima kasih kepada Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek) atas dukungan pendanaan yang diberikan dalam pelaksanaan penelitian ini. Peneliti juga menyampaikan apresiasi kepada Bapak Afriza Animawan Arifin selaku dosen pembimbing atas bimbingan, masukan, dan arahan yang konstruktif selama proses penelitian. Selain itu, peneliti mengucapkan terima kasih kepada seluruh anggota tim PKM-RSH The Dopva atas kerja sama dan kontribusi yang diberikan. Ucapan terima kasih juga disampaikan kepada semua pihak yang telah membantu kelancaran penelitian ini, meskipun tidak dapat disebutkan satu per satu.

Kontribusi Penulis

Tegar Adji Putra Pamungkas berperan sebagai peneliti utama yang bertanggung jawab atas seluruh kegiatan riset seperti perancangan penelitian, koordinasi pelaksanaan riset, pengumpulan dan analisis data, serta penulisan dan penyusunan artikel ilmiah. Adinda Zidna Fauzateni membantu dalam pengumpulan data penelitian, dan dokumentasi proses penelitian. Putri Ambar Sari membantu dalam pengumpulan dan analisis data penelitian. Afriza Animawan Arifin berperan sebagai dosen pembimbing yang memberikan arahan, bimbingan metodologis, dan masukan akademik selama proses penelitian hingga penyusunan artikel.

Konflik Kepentingan

Penulis menyatakan bahwa tidak terdapat konflik kepentingan, baik secara finansial maupun non-finansial, selama proses perencanaan, pelaksanaan, analisis data, hingga publikasi penelitian ini.

Pendanaan

Penelitian ini memperoleh pendanaan dari Program Kreativitas Mahasiswa Riset Sosial Humaniora (PKM-RSH) Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Kemendikbudristek).

REFERENSI

- Ahmad, S. (2026). *A User-Generated Content as a Driver of Trust: A Psychological Perspective on Peer Influence in Social Media*. <https://doi.org/10.20944/preprints202602.0127.v1>
- Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304–312. <https://doi.org/10.1016/j.chb.2014.05.046>
- Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLOS ONE*, 20(1), e0317232. <https://doi.org/10.1371/journal.pone.0317232>
- Balcombe, L. (2025). The Mental Health Impacts of Internet Scams. *International Journal of Environmental Research and Public Health*, 22(6), 938. <https://doi.org/10.3390/ijerph22060938>
- Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, 47(3), 391–408. <https://doi.org/10.1177/0004865814521224>
- Cazanis, A., Carminati, J.-Y., Chew, K., Cross, C., Ponsford, J., & Gould, K. R. (2025). “Falling into a Black Hole”: A Qualitative Exploration of the Lived Experiences of Cyberscam Victim-Survivors and Their Social Support Networks. *Victims & Offenders*, 1–20. <https://doi.org/10.1080/15564886.2025.2481267>
- Chu, Y., Liu, X., & Liu, C. (2025). The Role of Visual Cues in Online Reviews: How Image Complexity Shapes Review Helpfulness. *Journal of Theoretical and Applied Electronic Commerce Research*, 20(3), 181. <https://doi.org/10.3390/jtaer20030181>
- Cialdini, R. B. (2021). *Influence, new and expanded: The psychology of persuasion*. Harper Business.
- Federal Trade Commission. (2024, February). *Consumer Sentinel Network Data Book 2023*. <https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023>
- Federal Trade Commission. (2025, March 10). *New FTC Data Show Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024*. <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024>
- Frederick, S. (2005). Cognitive Reflection and Decision Making. *Journal of Economic Perspectives*, 19(4), 25–42. <https://doi.org/10.1257/089533005775196732>
- Geels, J., Graßl, P., Schraffenberger, H., Tanis, M., & Kleemans, M. (2024). Virtual lab coats: The effects of verified source information on social media post credibility. *PLOS ONE*, 19(5), e0302323. <https://doi.org/10.1371/journal.pone.0302323>
- Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic Decision Making. *Annual Review of Psychology*, 62(1), 451–482. <https://doi.org/10.1146/annurev-psych-120709-145346>
- Hancock, J. T. (2012). *Digital deception* (A. N. Joinson, K. Y. A. McKenna, T. Postmes, & U.-D. Reips, Eds.; Vol. 1). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199561803.013.0019>
- Hartini, S., & Hanafi, A. N. (2021). Pengaruh Kredibilitas dan Karakteristik Opinion Leader terhadap Behavioral Intention Konsumen pada Media Sosial Instagram. *Jurnal Maksipreneur: Manajemen, Koperasi, Dan Entrepreneurship*, 10(2), 211. <https://doi.org/10.30588/jmp.v10i2.704>
- Hoff, K. A., & Bashir, M. (2015). Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 57(3), 407–434. <https://doi.org/10.1177/0018720814547570>
- Hoffner, C. A., & Bond, B. J. (2022). Parasocial relationships, social media, & well-being. *Current Opinion in Psychology*, 45, 101306. <https://doi.org/10.1016/j.copsyc.2022.101306>
- Hoq, A., Facciani, M., & Weninger, T. (2025). *AI Credibility Signals Outrank Institutions and Engagement in Shaping News Perception on Social Media* (arXiv:2511.02370). arXiv. <https://doi.org/10.48550/arXiv.2511.02370>
- Javed, S., Rashidin, M. S., & Jian, W. (2024). Effects of heuristic and systematic cues on perceived content credibility of Sina Weibo influencers: The moderating role of involvement. *Humanities and Social Sciences Communications*, 11(1), 1635. <https://doi.org/10.1057/s41599-024-04107-w>
- Kahija, Y. F. L. (2017). *Penelitian fenomenologis: Jalan memahami pengalaman hidup*. Kanisius.
- Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
- Lenaini, I. (2021). *TEKNIK PENGAMBILAN SAMPEL PURPOSIVE DAN SNOWBALL SAMPLING*. 6(1).

- Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: Unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. *Safer Communities*, 23(4), 444–464. <https://doi.org/10.1108/SC-04-2024-0018>
- Liao, C. H., Hsieh, J.-K., & Kumar, S. (2024). Does the verified badge of social media matter? The perspective of trust transfer theory. *Journal of Research in Interactive Marketing*, 18(6), 1017–1033. <https://doi.org/10.1108/JRIM-10-2023-0339>
- Liu, H. (2025). Exploring the Effects of Social Influence on Online Ratings and Reviews. *Advances in Economics, Management and Political Sciences*, 158(1), 73–78. <https://doi.org/10.54254/2754-1169/2025.19703>
- Liu, X., & Zheng, X. (2024). The persuasive power of social media influencers in brand credibility and purchase intention. *Humanities and Social Sciences Communications*, 11(1), 15. <https://doi.org/10.1057/s41599-023-02512-1>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3), 709. <https://doi.org/10.2307/258792>
- McAllister, D. J. (1995). AFFECT- AND COGNITION-BASED TRUST AS FOUNDATIONS FOR INTERPERSONAL COOPERATION IN ORGANIZATIONS. *Academy of Management Journal*, 38(1), 24–59. <https://doi.org/10.2307/256727>
- Mehta, I. (2024, December 23). Pavel Durov says Telegram is now profitable. TechCrunch. <https://techcrunch.com/2024/12/23/pavel-durov-says-telegram-is-now-profitable/>
- Metzger, M. J., & Flanagin, A. J. (2013). Credibility and trust of information in online environments: The use of cognitive heuristics. *Journal of Pragmatics*, 59, 210–220. <https://doi.org/10.1016/j.pragma.2013.07.012>
- Moleong, L. J. (2019). *Metodologi penelitian kualitatif*. Remaja Rosdakarya.
- Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2024). Demystification and Actualisation of Data Saturation in Qualitative Research Through Thematic Analysis. *International Journal of Qualitative Methods*, 23, 16094069241229777. <https://doi.org/10.1177/16094069241229777>
- Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimization: A Systematic Review. *Journal of Police and Criminal Psychology*, 34(3), 231–245. <https://doi.org/10.1007/s11896-019-09334-5>
- Perez, S. (2024, October 15). Elon Musk's X still struggles to grow subscription revenue. TechCrunch. <https://techcrunch.com/2024/10/15/elon-musks-x-still-struggles-to-grow-subscription-revenue/>
- Sa'diyah, H. (2020). *KREDIBILITAS MEDIA SOSIAL INSTAGRAM @SUROBOYO.KU SEBAGAI MEDIUM PERMBERITAAN COVID – 19 MASYARAKAT KOTA SURABAYA*.
- Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology*, 13, 912242. <https://doi.org/10.3389/fpsyg.2022.912242>
- Sharot, T. (2011). The optimism bias. *Current Biology*, 21(23), R941–R945. <https://doi.org/10.1016/j.cub.2011.10.030>
- Sidiq, U., & Choiri, Moh. M. (2019). *Metode penelitian kualitatif di bidang pendidikan*. Nata Karya.
- Smith, J. A., Flowers, P., & Larkin, M. (2022). *Interpretative phenomenological analysis: Theory, method and research (2nd ed.)*. SAGE Publications.
- Sundar, S. S. (2008). The MAIN Model: A Heuristic Approach to Understanding Technology Effects on Credibility. *Digital Media*.
- Thorndike, E. L. (1920). A constant error in psychological ratings. *Journal of Applied Psychology*, 4(1), 25–29. <https://doi.org/10.1037/h0071663>
- Traberg, C. S., Harjani, T., Roozenbeek, J., & Van Der Linden, S. (2024). The persuasive effects of social cues and source effects on misinformation susceptibility. *Scientific Reports*, 14(1), 4205. <https://doi.org/10.1038/s41598-024-54030-y>
- Valori, I., Fan, Y., Jung, M. M., & Fairhurst, M. T. (2024). Propensity to trust shapes perceptions of comforting touch between trustworthy human and robot partners. *Scientific Reports*, 14(1), 6747. <https://doi.org/10.1038/s41598-024-57582-1>
- Xiao, M., Wang, M., Kulshrestha, A., & Mayer, J. (2023). *Account Verification on Social Media: User Perceptions and Paid Enrollment (Version 2)*. arXiv. <https://doi.org/10.48550/ARXIV.2304.14939>