

REPRESENTASI KEPERCAYAAN DALAM PESAN SCAM WHATSAPP BERKEDOK LAYANAN PERBANKAN (AWK TEUN A. VAN DIJK)

Darwin Effendi¹, Rika Sulistia², Winsi Aprilia³, Aisyah Dina S⁴, Sesilia Ceca O⁵,
Robiah⁶, Riska⁷, Rahma Puspita S⁸, Faza Utami⁹, Tiara Hati¹⁰, Salsabilah¹¹
Pendidikan Bahasa Indonesia, Fakultas Keguruan dan Ilmu Pendidikan,
Universitas PGRI Palembang

¹darwinpasca2010@gmail.com, ²rikasulistia94@gmail.com, ³apriawinsi@gmail.com, ⁴aisyadina268@gmail.com, ⁵sesiliacecaolv@gmail.com, ⁶robiah2056@gmail.com, ⁷rskaihy@gmail.com, ⁸rahmapuspita1290@gmail.com, ⁹faza2901@gmail.com, ¹⁰tiarahati031205@gmail.com, ¹¹salsabilahb64@gmail.com

ABSTRAK

Penelitian ini mengkaji bagaimana kepercayaan korban dibangun dan dimanipulasi dalam pesan scam WhatsApp berkedok layanan perbankan, menggunakan Analisis Wacana Kritis (AWK) Van Dijk pada dimensi teks, kognisi sosial, dan konteks sosial. Data berupa 16 screenshot percakapan nyata pelaku scam yang mengatasnamakan Bank UOB, BCA, dan Permata Intan dianalisis secara kualitatif. Empat modus penipuan ditemukan transaksi mencurigakan kartu kredit, permintaan QRIS, konfirmasi transaksi, dan undian berhadiah yang dibangun melalui struktur pembukaan-penutup sistematis, detail teknis spesifik, praanggapan otoritas (logo resmi, nama nasabah), serta koherensi kausal bernada ancaman. Keberhasilan penipuan bergantung pada skema mental korban bahwa bank dapat menghubungi nasabah secara mendesak via WhatsApp tanpa verifikasi, diperkuat relasi kuasa asimetris antara pelaku sebagai institusi dan korban sebagai nasabah individu. Temuan ini menegaskan perlunya verifikasi pesan melalui kanal resmi dan penguatan literasi keamanan digital masyarakat.

Kata kunci: Analisis Wacana Kritis, Van Dijk, kepercayaan, penipuan perbankan, WhatsApp

ABSTRACT

This study examines how victims' trust is established and manipulated in WhatsApp scam messages disguised as banking services, using Van Dijk's Critical Discourse Analysis (CDA) across the dimensions of text, social cognition, and social context. Data consisting of 16 screenshots of real conversations with scammers impersonating UOB Bank, BCA, and Permata Intan were analyzed qualitatively. Four fraud schemes were identified suspicious credit card transactions, QRIS requests, transaction confirmations, and prize draws constructed through a systematic introduction-body-conclusion structure, specific technical details, assumptions of authority (official logos, customer names), and causal coherence with a threatening tone. The success of the fraud relies on the victim's mental schema that banks can urgently contact customers via WhatsApp without verification, reinforced by the asymmetrical power relationship between the perpetrator as an institution and the victim as an individual customer.

These findings underscore the need for message verification through official channels and the strengthening of the public's digital security literacy.

Keywords: Critical Discourse Analysis, Van Dijk, trust, banking fraud, WhatsApp

A. PENDAHULUAN

Transformasi digital sektor keuangan secara global telah mengubah cara manusia berinteraksi dengan layanan perbankan secara mendasar. Kemunculan mobile banking, financial technology, dan platform pembayaran digital membuka akses keuangan yang lebih inklusif sekaligus menciptakan permukaan serangan baru yang dieksploitasi secara sistematis oleh pelaku kejahatan siber. Dalam lanskap ancaman siber kontemporer, social engineering strategi manipulasi psikologis yang memanfaatkan kepercayaan korban alih-alih celah teknis sistem menjadi metode serangan yang terus tumbuh dalam frekuensi maupun kecanggihan. Phishing, pretexting, dan impersonation sebagai turunan social engineering kini mendominasi insiden siber di berbagai negara, terutama di sektor keuangan yang menjadi sasaran paling menguntungkan bagi pelaku kejahatan digital.

Tren global tersebut berdampak langsung pada Indonesia sebagai salah satu pasar digital terbesar di Asia Tenggara. Badan Siber dan Sandi Negara (BSSN, 2023) dalam dokumen Lanskap Keamanan Siber Indonesia 2023 menegaskan bahwa phishing dan social engineering konsisten menjadi ancaman siber prioritas yang menyasar sektor keuangan nasional, di samping ancaman ransomware dan Advanced

Persistent Threat yang juga menunjukkan tren meningkat. Dampak ancaman tersebut terefleksi dalam data pengaduan konsumen yang dihimpun Otoritas Jasa Keuangan (OJK, 2024) sepanjang tahun 2023 hingga Januari 2024, OJK menerima 25.531 pengaduan konsumen, dengan 11.814 di antaranya berasal dari sektor perbankan. Angka ini mengonfirmasi bahwa pergeseran arena kejahatan dari kanal tradisional menuju platform digital bukan sekadar tren, melainkan realitas yang menuntut respons analitis yang memadai.

Dalam ekosistem platform digital yang beragam, WhatsApp muncul sebagai kanal yang paling rentan dieksploitasi untuk penipuan berkedok layanan perbankan. Data (We Are Social & Meltwater, 2023) menunjukkan bahwa 92,1% pengguna internet Indonesia menggunakan WhatsApp, menjadikannya aplikasi pesan dengan penetrasi tertinggi di negara ini. Tingginya penetrasi tersebut, dipadukan dengan tiga karakteristik inheren platform, membuat WhatsApp menjadi medium yang sangat efektif bagi pelaku scam: pertama, tingginya kepercayaan pengguna terhadap komunikasi berbasis pesan pribadi; kedua, kemudahan memanipulasi identitas pengirim melalui nama akun dan foto profil; ketiga, tidak adanya mekanisme verifikasi institusional yang tertanam secara bawaan dalam platform. Melalui

ketiga celah tersebut, pelaku mampu membangun persona sebagai representasi resmi lembaga keuangan terpercaya, sehingga korban tergiring untuk meyakini dan mematuhi setiap instruksi yang diberikan bahkan ketika instruksi tersebut secara logis seharusnya memicu kecurigaan.

Besarnya dampak fenomena ini mendorong sejumlah peneliti untuk mengkaji penipuan digital berbasis pesan dari berbagai sudut pandang. (Hidayah & Amran, 2023) menelaah modus penipuan social engineering pada nasabah perbankan melalui aplikasi WhatsApp secara yuridis-normatif, namun kajiannya berfokus pada dimensi hukum semata tanpa mengeksplorasi mekanisme wacana yang sesungguhnya bekerja di balik keberhasilan manipulasi tersebut. (Wulandari dkk., 2023) menerapkan analisis wacana model Van Dijk pada pesan penipuan giveaway yang mengatasnamakan figur publik di media sosial, tetapi objek kajiannya berupa pesan satu arah yang bersifat penyiaran berbeda secara fundamental dengan pesan scam real-time berbasis percakapan yang mengatasnamakan lembaga perbankan dan memiliki dinamika wacana yang jauh lebih kompleks. (Mujiyanto dkk., 2023) mengkaji kasus penipuan melalui Analisis Wacana Kritis Van Dijk pada pemberitaan media online, namun yang menjadi objek analisis adalah teks jurnalistik yang meliput peristiwa penipuan bukan teks wacana penipuan itu sendiri sebagaimana yang diproduksi pelaku dalam interaksi langsung dengan korban. Di sisi lain,

(Ariyanto & Rahmawati, 2025) melalui pendekatan linguistik forensik mengidentifikasi motif bahasa dalam pesan phishing di berbagai platform digital termasuk WhatsApp, menemukan bahwa strategi pseudo-authority, urgensi palsu, dan ancaman menjadi pola dominan dalam pesan yang menyamar sebagai institusi resmi; namun kajian tersebut berfokus pada klasifikasi bentuk dan makna bahasa secara umum tanpa menelaah keterkaitan ketiga dimensi wacana teks, kognisi sosial, dan konteks sosial dalam membangun kepercayaan korban.

Keempat kajian tersebut meninggalkan celah penelitian yang signifikan: belum ada penelitian yang secara spesifik membedah bagaimana kepercayaan korban direpresentasikan dan dimanipulasi melalui strategi wacana dalam percakapan scam WhatsApp berbahasa Indonesia yang mengatasnamakan lembaga perbankan, dengan menggunakan kerangka Analisis Wacana Kritis (AWK) Van Dijk secara komprehensif pada ketiga dimensi analisisnya teks, kognisi sosial, dan konteks sosial. Penelitian ini hadir untuk mengisi celah tersebut dengan membedah mekanisme linguistik dan ideologis yang bekerja di balik keberhasilan penipuan, bukan sekadar mendeskripsi modus operandinya. Konstruksi wacana yang terencana mulai dari pilihan makrostruktur teks dan strategi mikrolinguistik, model kognisi sosial yang melandasi produksi pesan, hingga eksploitasi relasi kuasa dan konteks sosial yang melingkupi praktik penipuan menjadi objek telaah yang membedakan penelitian ini dari kajian-

kajian sebelumnya. Hasil penelitian ini diharapkan memberikan kontribusi teoretis bagi pengembangan kajian AWK dalam wacana kejahatan digital berbahasa Indonesia, sekaligus menyediakan landasan empiris bagi peningkatan literasi keamanan digital masyarakat dan perumusan kebijakan perlindungan konsumen layanan keuangan yang lebih responsif terhadap ranah kejahatan siber saat ini.

B. METODOLOGI

Penelitian ini menggunakan metode kualitatif, dengan peneliti sebagai instrumen kunci dan analisis data bersifat induktif yang menekankan makna daripada generalisasi. Metode ini dipilih karena penelitian berfokus pada pemahaman makna serta bentuk representasi kepercayaan dalam pesan scam WhatsApp.

Data penelitian berupa 16 screenshot percakapan nyata antara pelaku scam dan calon korban melalui WhatsApp yang mengatasnamakan tiga lembaga perbankan UOB, BCA, dan Permata Intan dengan rentang waktu yang berbeda-beda. Identitas korban dan data finansial sensitif dianonimkan untuk menjaga prinsip anonimitas.

Pengumpulan data dilakukan melalui teknik dokumentasi, yakni mengumpulkan catatan peristiwa yang telah berlalu berupa tulisan, gambar, maupun karya monumental (Sugiyono, 2026), dalam bentuk screenshot percakapan yang diabadikan secara kronologis. Seluruh teks verbal kemudian ditranskripsikan ke dalam format teks untuk memudahkan

pengelompokan dan analisis. Selanjutnya, data dianalisis melalui tiga dimensi Van Dijk (1998, 2008, 2009, 2015) secara berurutan: (1) dimensi teks, meliputi makrostruktur (tema global), superstruktur (skema narasi), dan mikrostruktur (semantik, sintaksis, stilistik, dan retorika); (2) kognisi sosial, yaitu penafsiran model mental dan skema pengetahuan pelaku berdasarkan wacana pengakuan di akhir percakapan; serta (3) konteks sosial, yakni pengaitan temuan tekstual dengan relasi kuasa institusi perbankan-nasabah, kondisi keamanan siber perbankan nasional, dan implikasi ideologis.

Keabsahan data dijamin melalui triangulasi sumber, yaitu pengumpulan data dari berbagai sumber dengan teknik yang sama (Sugiyono, 2026), dengan membandingkan beberapa pesan scam WhatsApp dari sumber berbeda untuk menemukan kesamaan pola representasi kepercayaan.

C. HASIL DAN PEMBAHASAN

Penelitian ini mengidentifikasi dan menganalisis wacana penipuan pada 16 screenshot percakapan WhatsApp berbasis perbankan yang dikategorikan ke dalam empat modus penipuan UOB, QRIS BCA, Permata Bank, hingga undian hadiah BCA/Mandiri/BRI melalui tiga dimensi AWK Van Dijk yaitu (1) dimensi teks yang meliputi struktur makro, superstruktur, dan struktur mikro (semantik, sintaksis, stilistik, retorika); (2) dimensi kognisi sosial; serta (3) dimensi konteks sosial.

1. Struktur Makro (Tematik: Topik)

Struktur makro menggambarkan inti pesan yang ingin disampaikan (Van Dijk, 1998). Ditemukan empat topik utama:

Tabel 1. Topik Pesan Penipuan WhatsApp

N o	Kode Data	Topik	Isi Pesan
1	D1/W A-UOB	Transaksi mencurigakan kartu kredit	Pemberitahuan transaksi pembelian pulsa di Tokopedia Rp3.025.000 mengatasnamakan Bank UOB
2	D2/W A-QRIS	Permintaan pembayaran QRIS	Pelaku meminta korban memfoto kode QRIS BCA dengan dalih tidak bisa transfer via Visa
3	D3/W A-Permata	Konfirmasi transaksi kartu kredit	Klaim dari Permata Bank atas transaksi di MERCHANT Online MAMIKOS senilai Rp7.003.500
4	D4/W A-Undian	Undian berhadiah dari bank	Klaim rekening terpilih mendapat uang tunai Rp100 juta atas nama BCA, Mandiri, atau BRI

Keempat topik seluruhnya memanfaatkan nama lembaga perbankan resmi sebagai alat legitimasi. Topik pertama paling kompleks karena memadukan tekanan waktu, ancaman kerugian, dan bujukan merespons cepat, sementara topik keempat menunjukkan adaptabilitas pelaku yang mengubah nama bank sesuai respons korban sebagai bentuk manipulasi tingkat lanjut.

2. Superstruktur (Skematik: Skema)

Superstruktur merupakan kerangka pembuka-isi-penutup (Van Dijk, 1998), yang hadir konsisten pada seluruh data:

Tabel 2. Skema Pesan Penipuan WhatsApp (D1/WA-UOB)

Bagian	Tuturan
Pembuka	"Dari bank UOB, apakah benar kami terhubung dengan nasabah kami atas nama..."
Isi	"...di kartu kredit Anda dengan awalan nomor 4219 dan akhiran 3477, ada transaksi tidak wajar pembelian pulsa di Tokopedia sebesar Rp3.025.000..."
Penutup	"Baik, akan kami hubungi dan kirimkan SMS dari UOB untuk pemblokiran dan pembatalan transaksi"

Pembuka membangun kredibilitas dengan menyebut nama lembaga dan/atau nasabah pada D3/WA-Permata bahkan menggunakan nama lengkap nasabah sejak kalimat pertama untuk kesan urgensi. Isi memuat detail teknis spesifik (nomor kartu, nama merchant, nominal, tanggal), sedangkan penutup selalu

berisi instruksi atau ancaman yang mendesak respons segera.

3. Struktur Mikro

3.1 Semantik

a) Latar dan Detail

Latar adalah pembenaran atas gagasan yang diajukan, sedangkan detail adalah informasi spesifik yang membangun kedalaman teks (Van Dijk, 2009):

Tabel 3. Latar dan Detail Pesan Penipuan

Kode Data	Latar	Detail Pendukung
D1/W A-UOB	Hari libur bank ("...sampe Bank UOB hari libur bank menghub saya?")	Nomor kartu sebagian (421...477), nominal Rp3.025.000, nama merchant
D2/W A-QRIS	Lokasi di Malaysia ("syaa msih di malay kk, tf lewat visa gada fitur...")	Foto kartu QRIS BCA asli sebagai bukti visual
D3/W A-Permata	-	Tanggal transaksi (18/02/2026), nama merchant MAMIKO S, nominal Rp7.003.500
D4/W A-	Pelaku menyesuaikan	-

Undian	latar bank secara dinamis (BCA→Mandiri →BRI)	
--------	--	--

Latar membangun plausibilitas atas tindakan yang sebenarnya tidak lazim secara procedural misalnya menjelaskan mengapa "bank" menghubungi via WhatsApp di hari libur (D1) atau mengapa transfer harus lewat QRIS (D2). Detail teknis yang spesifik memperkuat kesan bahwa pengirim benar-benar memiliki akses ke data perbankan korban, sehingga pesan tampak sebagai notifikasi resmi.

b) Maksud

Elemen maksud melihat tujuan tersembunyi di balik teks (Van Dijk, 2008):

Tabel 4. Maksud Pesan Penipuan

Kode Data	Tuturan	Maksud Tersembunyi
D1/W A-UOB	"Jika bukan transaksi anda maka sebaiknya kartu anda diblokir..."	Mendorong korban menyerahkan kode OTP dengan dalih pemblokiran kartu
D2/W A-QRIS	"fotoin aja qris bca nya kak"	Mendapatkan foto QRIS aktif korban untuk disalahgunakan
D3/W A-Permata	"Mohon konfirmasi, apakah benar transaksi tersebut..."	Memancing respons korban sebagai pintu masuk manipulasi lanjutan

D4/WA-Undian	"...rekening anda terpilih dapat uang tunai 100 jt. Info lanjut hub 021-30304066"	Mengarahkan korban menghubungi nomor palsu untuk memeras biaya admin fiktif
--------------	---	---

Seluruh maksud tersembunyi bertujuan sama: memperoleh akses ke akun atau aset finansial korban, melalui tiga mekanisme OTP (D1), data QRIS (D2), atau biaya administrasi fiktif (D4).

c) Praanggapan

Praanggapan memberi pernyataan tepercaya yang tidak perlu dipertanyakan pembaca (Van Dijk, 2009):

Tabel 5. Praanggapan Pesan Penipuan

Kode Data	Praanggapan
D1/WA-UOB	Foto profil berlogo UOB resmi + sebagian nomor kartu kredit korban, ini memberikan kesan pengirim adalah pihak bank sah
D3/WA-Permata	Nama lengkap nasabah + gaya bahasa surat resmi, menunjukkan kesan pesan dari divisi fraud Permata Bank
D2/WA-QRIS	Foto kartu QRIS BCA asli, membuat kesan transaksi legitim
D4/WA-Undian	"Oh oke klo gitu kami dari bank mandiri", memberikan kesan pengirim mengetahui data rekening korban

Praanggapan dibangun lewat kombinasi elemen visual (logo, QRIS

asli) dan linguistik (nama nasabah, sebagian nomor rekening) sehingga korban sulit mempertanyakan otoritas pengirim secara spontan. Pada D4, praanggapan ini dibangun secara adaptif pelaku sebenarnya tidak memiliki data korban, namun berpura-pura memilikinya dengan mengikuti informasi yang justru diberikan korban sendiri.

d) Nominalisasi

Nominalisasi mengubah kata kerja menjadi kata benda untuk memanipulasi persepsi (Van Dijk, 2008):

Tabel 6. Nominalisasi Pesan Penipuan

Kode Data	Nominalisasi	Tuturan
D1/WA-UOB	Pemblokiran & pembatalan	"...untuk melakukan pemblokiran dan pembatalan transaksi"
D1/WA-UOB	Pembelian	"...transaksi yg tidak wajar pembelian pulsa..."
D3/WA-Permata	Konfirmasi	"Mohon konfirmasi, apakah benar transaksi tersebut..."
D3/WA-Permata	Keamanan	"Untuk keamanan, saat ini transaksi... telah kami hold"

Nominalisasi seperti "pemblokiran", "konfirmasi", dan "keamanan" menciptakan kesan bahwa

situasi yang dihadapi korban adalah prosedur administratif perbankan yang sah dan mendesak, bukan jebakan penipuan.

3.2 Sintaksis

a) Bentuk Kalimat dan Koherensi

Bentuk kalimat berkaitan dengan logika kausalitas, sedangkan koherensi adalah perkaitan antarproposisi yang membentuk kesatuan makna (Van Dijk, 1998, 2009):

Tabel 7. Bentuk Kalimat dan Koherensi Pesan Penipuan

Kode Data	Tuturan	Bentuk & Koherensi
D1/WA-UOB	"Jika bukan transaksi anda maka sebaiknya kartu anda diblokir..."	Kalimat kompleks bersyarat (jika...maka) termasuk koherensi kausal/syarat berkesan prosedural resmi
D1/WA-UOB	"...jika tidak anda batalkan kami pastikan akan mengurus habis limite kredit anda dan akan merambat ke perbankan lain nya"	Koherensi kausal ancaman (jika...akan) menjadi bentuk paling kuat memaksa respons segera
D1/WA-UOB	"Mohon untuk tidak menyia2kan waktu kami ya"	Kalimat imperatif pendek sehingga menekan

	bu" / "Transaksi sedang urgent"	ruang berpikir kritis korban
D3/WA-Permat a	"Mohon konfirmasi, apakah benar transaksi tersebut dilakukan oleh Bapak/Ibu"	Kalimat tanya retorik dengan koherensi waktu ("saat ini... telah kami hold")
D4/WA-Undian	"Oh oke klo gitu kami dari bank mandiri" / "Oh itu juga gpp, kami dari BRI"	Kalimat deklaratif dengan koherensi adaptif menjadi klaim menyesuaikan respons korban

Temuan paling menonjol adalah koherensi kausal ancaman pada D1 ("...jika tidak anda batalkan...akan mengurus habis limite kredit") diposisikan setelah kepercayaan terbangun di awal percakapan, sehingga dampak psikologisnya maksimal. Kombinasi kalimat kompleks bersyarat dengan imperatif pendek menciptakan logika sebab dan akibat yang terasa resmi sekaligus mendesak, mereduksi ruang berpikir kritis korban.

b) Kata Ganti

Kata ganti menunjukkan posisi seseorang dalam wacana (Van Dijk, 2008):

Tabel 8. Kata Ganti Pesan Penipuan

Kode Data	Kata Ganti	Fungsi Strategis
-----------	------------	------------------

D1/W A- UOB	"kami" vs "anda/Bu"	Kontras institusional personal: "kami" membangun kesan kelembagaan resmi, sapaan personal menempatkan korban sebagai nasabah yang "perlu dilindungi"
D3/W A- Perma ta	"Bapak/Ibu"	Sapaan formal surat resmi untuk legitimasi
D2/W A- QRIS	"kak"	Kesan keakraban, menurunkan kewaspadaan
D4/W A- Undia n	"kami dari BCA/Mandiri/ BRI"	"Kami" dan nama bank bergantian sebagai strategi adaptasi identitas

Kontras antara "kami" institusional dan sapaan personal kepada korban menciptakan relasi kekuasaan asimetris: pelaku berposisi sebagai otoritas, korban sebagai pihak yang wajib kooperatif.

3.3 Stilistik (Leksikon)

Stilistik berfokus pada pilihan kata dari berbagai kemungkinan yang ada (Van Dijk, 2008):

Tabel 9. Leksikon Pesan Penipuan

Leksikon	Kode Data	Fungsi Manipulatif
"tidak wajar" / "scamming"	D1	Membangun kepanikan
"urgent" / "secepatnya"	D1	Menciptakan tekanan waktu
"kami sanggakan" / "kami proses"	D1	Leksikon prosedural untuk legitimasi institusional
"hold" / "konfirmasi"	D3	Istilah teknis perbankan resmi
"terpilih" / "mendapatkan"	D4	Leksikon kemenangan, menurunkan kewaspadaan
"kak" / "gpp"	D2	Leksikon akrab untuk membangun kepercayaan personal

Pelaku menggunakan dua register secara bergantian: formal perbankan untuk legitimasi, dan informal percakapan untuk kedekatan personal strategi hibrida yang efektif menyamarkan niat penipuan.

3.4 Retoris

a) Grafis

Elemen grafis mencakup huruf tebal, kapital, dan elemen visual lain (Van Dijk, 1998):

Tabel 10. Grafis Pesan Penipuan

Kode Data	Elemen Grafis	Keterangan
D3/WA- Permata	Huruf tebal pada	"...telah kami hold" dan "Mohon

	kalimat krusial	konfirmasi..." dicetak tebal mengikuti konvensi surat resm
D3/WA-Permata	Huruf kapital	"MERCHANT Online MAMIKOS" menegaskan detail agar tampak resmi
D2/WA-QRIS	Gambar QRIS asli	Foto kartu QRIS BCA + demonstrasi penggunaan sebagai bukti visual
D1/WA-UOB	Foto profil berlogo resmi	Logo Bank UOB sebagai identitas institusional

Elemen grafis logo resmi, gambar QRIS asli, huruf tebal dan kapital menunjukkan sofistikasi visual yang melampaui manipulasi teks semata, memperkuat ilusi legitimasi institusional.

b) Metafora Ekspresi

Metafora ekspresi menjadi landasan berpikir atau pembenaran atas pendapat yang disampaikan (Van Dijk, 1998):

Tabel 11. Metafora Ekspresi Pesan Penipuan

Kode Data	Metafora	Analisis
D1/WA-UOB	"menguras habis limite kredit"	Metafora cairan untuk kehilangan finansial dramatis
D1/WA-UOB	"merambat ke	Metafora penyebaran penyakit,

	perbankan lain nya"	memperbesar skala ancaman
D1/WA-UOB	"sudah dipastikan sdh di scamming oleh hacker perbankan"	Metafora serangan digital, menciptakan rasa takut mendalam
D3/WA-Permata	"hold"	Metafora fisik untuk transaksi digital, kesan teknis dan sah

"Menguras habis" dan "merambat" bekerja sinergis membangun narasi bencana finansial berskala besar dan progresif strategi retorik yang memicu respons berbasis ketakutan yang melumpuhkan daya pikir kritis korban.

4. Dimensi Kognisi Sosial

Dimensi kognisi sosial mengungkap skema pengetahuan yang dieksploitasi pelaku dari benak korban: kepercayaan bahwa pihak bank dapat dan akan menghubungi nasabah langsung via WhatsApp untuk urusan transaksi mendesak, bahkan di hari libur (D1) padahal secara prosedural hal ini tidak lazim. Skema mental ini diperkuat oleh kebiasaan masyarakat merespons cepat setiap notifikasi transaksi tanpa verifikasi independen ke saluran resmi bank. Eksploitasi ini tampak paling jelas pada D4/WA-Undian: pelaku sesungguhnya tidak memiliki data rekening korban, namun secara adaptif menyesuaikan klaim nama bank (BCA/Mandiri/BRI) mengikuti informasi yang justru diberikan korban sendiri menunjukkan

bahwa keberhasilan penipuan bergantung pada model mental korban tentang "bagaimana bank semestinya berkomunikasi", bukan pada data aktual yang dimiliki pelaku.

5. Dimensi Konteks Sosial

Dimensi konteks sosial menunjukkan relasi kuasa asimetris antara pelaku yang memosisikan diri sebagai institusi ("kami") dan korban yang diposisikan sebagai nasabah individu yang wajib kooperatif. Relasi ini beroperasi dalam konteks sosial yang lebih luas: tingginya ketergantungan masyarakat Indonesia terhadap layanan perbankan digital, minimnya literasi keamanan siber, serta ketimpangan akses informasi antara institusi keuangan dan nasabah awam. Dibandingkan modus penipuan yang lebih sederhana seperti giveaway selebriti (Wulandari dkk., 2023), penipuan berkedok perbankan dalam penelitian ini memanfaatkan terminologi teknis, elemen visual resmi, dan strategi psikologis berbasis ketakutan secara jauh lebih sistematis menjadikannya lebih berbahaya dan sulit dideteksi oleh korban awam.

D. KESIMPULAN

Berdasarkan analisis AWK Van Dijk terhadap dokumentasi percakapan scam WhatsApp berkedok layanan perbankan, dapat disimpulkan bahwa kepercayaan korban dibangun dan dimanipulasi melalui tiga dimensi yang saling berkaitan. Pada dimensi teks, pelaku mengonstruksi pesan dengan struktur pembuka-isi-penutup yang sistematis, memadukan detail teknis spesifik, praanggapan otoritas (logo

resmi, nama nasabah), koherensi kausal bernada ancaman, serta perpaduan register formal dan informal sehingga tercipta ilusi legitimasi institusional sekaligus tekanan psikologis pada korban. Pada dimensi kognisi sosial, keberhasilan penipuan bergantung pada skema mental korban bahwa bank dapat menghubungi nasabah secara mendesak via WhatsApp tanpa verifikasi independen, bahkan ketika pelaku sebenarnya sama sekali tidak memiliki data korban, sebagaimana terlihat pada modus undian berhadiah yang secara adaptif menyesuaikan nama bank sesuai respons korban sendiri. Pada dimensi konteks sosial, relasi kuasa asimetris antara pelaku yang berposisi sebagai institusi ("kami") dan korban sebagai nasabah individu diperkuat oleh tingginya ketergantungan masyarakat pada layanan perbankan digital serta rendahnya literasi keamanan siber, sehingga modus penipuan berkedok perbankan ini lebih sistematis dan sulit dideteksi dibandingkan modus penipuan sederhana seperti giveaway selebriti.

Dari temuan tersebut, masyarakat disarankan untuk selalu memverifikasi setiap pesan yang mengatasmakan bank melalui kanal resmi sebelum merespons, terutama jika pesan memuat tekanan waktu atau permintaan kode OTP dan QRIS. Lembaga perbankan disarankan memperkuat edukasi publik mengenai pola wacana penipuan semacam ini serta menegaskan kembali bahwa data sensitif seperti OTP tidak pernah diminta melalui WhatsApp. Penelitian selanjutnya dapat memperluas objek kajian pada platform digital lain atau

modus penipuan berkedok institusi non-perbankan untuk memperkaya pemahaman strategi wacana kejahatan digital di Indonesia. Selain itu, sejalan dengan (Widyawati dkk., 2026) yang menerapkan struktur wacana Van Dijk pada iklan layanan masyarakat BCA bertema kewaspadaan penipuan, penelitian selanjutnya juga dapat membandingkan strategi wacana antara pesan scam dan materi edukasi anti-penipuan resmi untuk mengukur efektivitas pesan preventif tersebut dalam membentuk kewaspadaan masyarakat.

DAFTAR PUSTAKA

- Ariyanto, Z. R., & Rahmawati, L. E. (2025). The form and meaning of language motifs in phishing crimes: A forensic linguistic study. *LITE: Jurnal Bahasa, Sastra, dan Budaya*, 21(1), 270–289. Doi:10.33633/lite.v21i1.11463
- Badan Siber dan Sandi Negara [BSSN]. (2023). *Lanskap Keamanan Siber Indonesia 2023*. Jakarta: BSSN. Diakses dari <https://www.bssn.go.id/wp-content/uploads/2024/03/Lanska-p-Keamanan-Siber-Indonesia-2023.pdf>
- Hidayah, N., & Amran. (2023). Tinjauan yuridis tindak pidana penipuan social engineering pada nasabah perbankan melalui aplikasi chat WhatsApp. *Jurnal Pustaka Cendekia Hukum dan Ilmu Sosial*, 1(1), 116–127. Diakses dari <https://pchukumsosial.org/>
- Mujiyanto, H., Hendrawan, H., & Sadiyah, H. (2023). Analisis wacana kritis pemberitaan kasus penipuan di media online Kompas.com. *Jurnal Komunikasi Universitas Garut: Hasil Pemikiran dan Penelitian*, 9(1), 1016–1030. Doi:10.52434/JK.V9i1.2464
- Ni Wayan Dian Ari Widyawati, I Wayan Pastika, & Made Sri Satyawati. (2026). Analisis Wacana Kritis pada Iklan Layanan Masyarakat BCA “Modus Penipuan Makin Agak Laen, Kasih Tau yang Laen!”. *Jurnal Bastra (Bahasa dan Sastra)*, 11(3), 1597–1605. Doi:10.36709/bastra.v11i3.2566
- Otoritas Jasa Keuangan [OJK]. (2024). Sektor jasa keuangan yang kuat dan stabil untuk mendukung pertumbuhan ekonomi yang berkelanjutan [Siaran pers]. Diakses dari <https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/Sektor-Jasa-Kuangan-yang-Kuat-dan-Stabil-untuk-Mendukung-Pertumbuhan-Ekonomi-yang-Berkelanjutan.aspx>
- Sugiyono. (2026). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.
- Van Dijk, T. A. (1998). *News as Discourse*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Van Dijk, T. A. (2008). *Discourse and Context: A Sociocognitive Approach*. Cambridge: Cambridge University Press. Diakses dari <https://discourses.org/wp-content/uploads/2022/06/Teun-A.-van-Dijk-2008-Discourse-and-Context-A-Sociocognitive-Approach.pdf>

- Van Dijk, T. A. (2009). *Society and Discourse: How Social Contexts Influence Text and Talk*. Cambridge: Cambridge University Press. Diakses dari <https://discourses.org/wp-content/uploads/2022/06/Teun-A.-van-Dijk-2009-Society-And-Discourse.-How-Social-Contexts-Influence-Text-And-Talk.pdf>
- Van Dijk, T. A. (2015). Critical discourse studies: A sociocognitive approach. Dalam R. Wodak & M. Meyer (Eds.), *Methods of Critical Discourse Studies* (3rd ed., pp. 62–85). London: Sage.
- We Are Social, & Meltwater. (2023). *Digital 2023: Indonesia*. DataReportal. Diakses dari <https://datareportal.com/reports/digital-2023-indonesia>
- Wulandari, S., Budiawan, R. Y. S., & Mualafina, R. F. (2023). Analisis wacana model Van Dijk pada pesan penipuan atas nama Baim Wong di media sosial. *Sintesis*, 17(1), 1–11. Doi:10.24071/sin.v17i1.5395